# ZyWALL 2 Plus

*Internet Security Appliance*

# User's Guide

Version 4.03
12/2007
Edition 1

ZyXEL
www.zyxel.com

# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the ZyWALL using the web configurator or System Management Terminal (SMT). You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.

It is recommended you use the web configurator to configure the ZyWALL.

- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

## User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

# Document Conventions

### Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

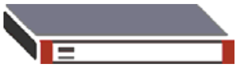
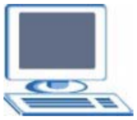
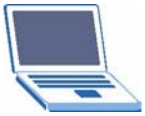
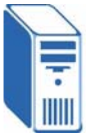
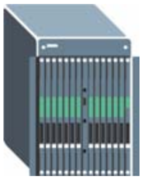
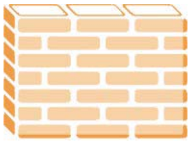
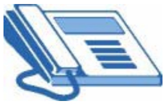
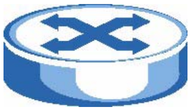
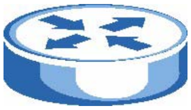
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

### Syntax Conventions

- The ZyWALL 2 Plus may be referred to as the "ZyWALL", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

## Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyWALL icon is not an exact representation of your device.

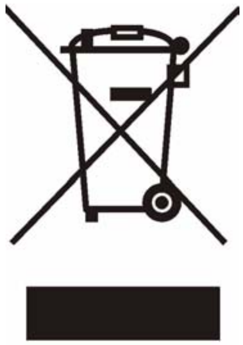
| | | |
|---|---|---|
| ZyWALL<br> | Computer<br> | Notebook computer<br> |
| Server<br> | DSLAM<br> | Firewall<br> |
| Telephone<br> | Switch<br> | Router<br> |

# Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.

This product is recyclable. Dispose of it properly.



# Contents Overview

**Introduction and Registration ......................................................................................45**

Getting to Know Your ZyWALL ........................................................................................ 47
Introducing the Web Configurator .................................................................................... 51
Wizard Setup .................................................................................................................... 69
Tutorials ........................................................................................................................... 89
Registration .................................................................................................................... 127

**Network ...........................................................................................................................131**

LAN Screens .................................................................................................................. 133
Bridge Screens ............................................................................................................... 145
WAN Screens ................................................................................................................. 151
DMZ Screens .................................................................................................................. 171
Wireless LAN .................................................................................................................. 181

**Security ..........................................................................................................................189**

Firewall ........................................................................................................................... 191
Content Filtering Screens ............................................................................................... 223
Content Filtering Reports ................................................................................................ 245
IPSec VPN ...................................................................................................................... 253
Certificates ...................................................................................................................... 295
Authentication Server ..................................................................................................... 323

**Advanced .......................................................................................................................329**

Network Address Translation (NAT) ............................................................................... 331
Static Route .................................................................................................................... 347
Bandwidth Management ................................................................................................. 351
DNS ................................................................................................................................ 365
Remote Management ...................................................................................................... 377
UPnP .............................................................................................................................. 399
Custom Application ........................................................................................................ 409
ALG Screen .....................................................................................................................411

**Logs and Maintenance .................................................................................................417**

Logs Screens ................................................................................................................. 419
Maintenance ................................................................................................................... 447

**SMT** .......... **465**

Introducing the SMT .......... 467
SMT Menu 1 - General Setup .......... 475
WAN and Dial Backup Setup .......... 481
LAN Setup .......... 491
Internet Access .......... 497
DMZ Setup .......... 501
Wireless Setup .......... 505
Remote Node Setup .......... 509
IP Static Route Setup .......... 519
Network Address Translation (NAT) .......... 521
Introducing the ZyWALL Firewall .......... 539
Filter Configuration .......... 541
SNMP Configuration .......... 557
System Information & Diagnosis .......... 559
Firmware and Configuration File Maintenance .......... 571
System Maintenance Menus 8 to 10 .......... 587
Remote Management .......... 595
Call Scheduling .......... 599

**Troubleshooting and Specifications** .......... **603**

Troubleshooting .......... 605
Product Specifications .......... 613

**Appendices and Index** .......... **619**

# Table of Contents

About This User's Guide .......................................... 3

Document Conventions .......................................... 4

Safety Warnings .......................................... 6

Contents Overview .......................................... 7

Table of Contents .......................................... 9

List of Figures .......................................... 27

List of Tables .......................................... 39

Part I: Introduction and Registration .......................................... 45

Chapter 1
Getting to Know Your ZyWALL .......................................... 47

- 1.1 ZyWALL Internet Security Appliance Overview .......................................... 47
- 1.2 Applications for the ZyWALL .......................................... 47
  - 1.2.1 Secure Broadband Internet Access via Cable or DSL Modem .......................................... 47
  - 1.2.2 VPN Application .......................................... 48
- 1.3 Ways to Manage the ZyWALL .......................................... 48
- 1.4 Good Habits for Managing the ZyWALL .......................................... 49
- 1.5 LEDs .......................................... 49

Chapter 2
Introducing the Web Configurator .......................................... 51

- 2.1 Web Configurator Overview .......................................... 51
- 2.2 Accessing the ZyWALL Web Configurator .......................................... 51
- 2.3 Resetting the ZyWALL .......................................... 53
  - 2.3.1 Procedure To Use The Reset Button .......................................... 53
  - 2.3.2 Uploading a Configuration File Via Console Port .......................................... 53
- 2.4 Navigating the ZyWALL Web Configurator .......................................... 54
  - 2.4.1 Title Bar .......................................... 54
  - 2.4.2 Main Window .......................................... 55
  - 2.4.3 HOME Screen: Router Mode .......................................... 55
  - 2.4.4 HOME Screen: Bridge Mode .......................................... 57
  - 2.4.5 Navigation Panel .......................................... 60

2.4.6 Port Statistics .......... 64
2.4.7 DHCP Table Screen .......... 65
2.4.8 VPN Status .......... 66
2.4.9 Bandwidth Monitor .......... 67

**Chapter 3**
**Wizard Setup .......... 69**

3.1 Wizard Setup Overview .......... 69
3.2 Internet Access .......... 70
3.2.1 ISP Parameters .......... 70
3.2.2 Internet Access Wizard: Second Screen .......... 75
3.2.3 Internet Access Wizard: Registration .......... 76
3.3 VPN Wizard Gateway Setting .......... 79
3.4 VPN Wizard Network Setting .......... 80
3.5 VPN Wizard IKE Tunnel Setting (IKE Phase 1) .......... 82
3.6 VPN Wizard IPSec Setting (IKE Phase 2) .......... 83
3.7 VPN Wizard Status Summary .......... 85
3.8 VPN Wizard Setup Complete .......... 87

**Chapter 4**
**Tutorials .......... 89**

4.1 Security Settings for VPN Traffic .......... 89
4.1.1 Firewall Rule for VPN Example .......... 89
4.1.2 Configuring the VPN Rule .......... 90
4.1.3 Configuring the Firewall Rules .......... 93
4.2 Using NAT with Multiple Public IP Addresses .......... 97
4.2.1 Example Parameters and Scenario .......... 97
4.2.2 Configuring the WAN Connection with a Static IP Address .......... 98
4.2.3 Public IP Address Mapping .......... 101
4.2.4 Forwarding Traffic from the WAN to a Local Computer .......... 105
4.2.5 Allow WAN-to-LAN Traffic through the Firewall .......... 107
4.2.6 Testing the Connections .......... 114
4.3 Using NAT with Multiple Game Players .......... 114
4.4 How to Manage the ZyWALL’s Bandwidth .......... 115
4.4.1 Example Parameters and Scenario .......... 115
4.4.2 Configuring Bandwidth Management Rules .......... 116
4.5 Configuring Content Filtering .......... 120
4.5.1 Enable Content Filtering .......... 120
4.5.2 Block Categories of Web Content .......... 121
4.5.3 Assign Bob’s Computer a Specific IP Address .......... 123
4.5.4 Create a Content Filter Policy for Bob .......... 123
4.5.5 Set the Content Filter Schedule .......... 124
4.5.6 Block Categories of Web Content for Bob .......... 125

**Chapter 5**
**Registration ............................................................ 127**

5.1 myZyXEL.com overview ............................................................ 127
    5.1.1 Content Filtering Subscription Service ............................................................ 127
5.2 Registration ............................................................ 128
5.3 Service ............................................................ 129

**Part II: Network............................................................ 131**

**Chapter 6**
**LAN Screens............................................................ 133**

6.1 LAN, WAN and the ZyWALL ............................................................ 133
6.2 IP Address and Subnet Mask ............................................................ 133
    6.2.1 Private IP Addresses ............................................................ 134
6.3 DHCP ............................................................ 135
    6.3.1 IP Pool Setup ............................................................ 135
6.4 RIP Setup ............................................................ 135
6.5 Multicast ............................................................ 135
6.6 WINS ............................................................ 136
6.7 LAN ............................................................ 136
6.8 LAN Static DHCP ............................................................ 139
6.9 LAN IP Alias ............................................................ 140
6.10 LAN Port Roles ............................................................ 142

**Chapter 7**
**Bridge Screens............................................................ 145**

7.1 Bridge Loop ............................................................ 145
7.2 Spanning Tree Protocol (STP) ............................................................ 146
    7.2.1 Rapid STP ............................................................ 146
    7.2.2 STP Terminology ............................................................ 146
    7.2.3 How STP Works ............................................................ 146
    7.2.4 STP Port States ............................................................ 147
7.3 Bridge ............................................................ 147
7.4 Bridge Port Roles ............................................................ 149

**Chapter 8**
**WAN Screens............................................................ 151**

8.1 WAN Overview ............................................................ 151
8.2 TCP/IP Priority (Metric) ............................................................ 151
8.3 WAN Route ............................................................ 151
8.4 WAN IP Address Assignment ............................................................ 153

8.5 DNS Server Address Assignment ........ 153
8.6 WAN MAC Address ........ 154
8.7 WAN ........ 154
  8.7.1 WAN Ethernet Encapsulation ........ 154
  8.7.2 PPPoE Encapsulation ........ 157
  8.7.3 PPTP Encapsulation ........ 160
8.8 Traffic Redirect ........ 163
8.9 Configuring Traffic Redirect ........ 164
8.10 Configuring Dial Backup ........ 165
8.11 Advanced Modem Setup ........ 168
  8.11.1 AT Command Strings ........ 168
  8.11.2 DTR Signal ........ 168
  8.11.3 Response Strings ........ 169
8.12 Configuring Advanced Modem Setup ........ 169

**Chapter 9**
**DMZ Screens ........ 171**

9.1 DMZ ........ 171
9.2 Configuring DMZ ........ 171
9.3 DMZ Static DHCP ........ 174
9.4 DMZ IP Alias ........ 175
9.5 DMZ Public IP Address Example ........ 177
9.6 DMZ Private and Public IP Address Example ........ 177
9.7 DMZ Port Roles ........ 178

**Chapter 10**
**Wireless LAN ........ 181**

10.1 Wireless LAN Introduction ........ 181
10.2 Configuring WLAN ........ 181
10.3 WLAN Static DHCP ........ 184
10.4 WLAN IP Alias ........ 185
10.5 WLAN Port Roles ........ 187

**Part III: Security ........ 189**

**Chapter 11**
**Firewall ........ 191**

11.1 Firewall Overview ........ 191
11.2 Packet Direction Matrix ........ 192
11.3 Packet Direction Examples ........ 193
  11.3.1 To VPN Packet Direction ........ 195

11.3.2 From VPN Packet Direction ..................................................................... 196
11.3.3 From VPN To VPN Packet Direction ........................................................... 198
11.4 Security Considerations .................................................................................... 199
11.5 Firewall Rules Example ..................................................................................... 200
11.6 Asymmetrical Routes ......................................................................................... 201
11.6.1 Asymmetrical Routes and IP Alias ............................................................ 202
11.7 Firewall Default Rule (Router Mode) ................................................................. 202
11.8 Firewall Default Rule (Bridge Mode) ................................................................ 204
11.9 Firewall Rule Summary ..................................................................................... 206
11.9.1 Firewall Edit Rule ...................................................................................... 208
11.10 Anti-Probing .....................................................................................................211
11.11 Firewall Thresholds ......................................................................................... 212
11.11.1 Threshold Values .................................................................................... 213
11.12 Threshold Screen ............................................................................................. 213
11.13 Service ............................................................................................................. 215
11.13.1 Firewall Edit Custom Service ................................................................. 216
11.14 My Service Firewall Rule Example .................................................................. 217

**Chapter 12**
**Content Filtering Screens ..................................................................................223**

12.1 Content Filtering Overview ................................................................................ 223
12.1.1 Restrict Web Features ............................................................................... 223
12.1.2 Create a Filter List ..................................................................................... 223
12.1.3 Customize Web Site Access ...................................................................... 223
12.2 Content Filtering with an External Database .................................................... 223
12.3 Content Filter General Screen .......................................................................... 224
12.4 Content Filter Policy ......................................................................................... 227
12.5 Content Filter Policy: General ........................................................................... 229
12.6 Content Filter Policy: External Database .......................................................... 230
12.7 Content Filter Policy: Customization ................................................................. 237
12.8 Content Filter Policy: Schedule ......................................................................... 239
12.9 Content Filter Object ......................................................................................... 240
12.10 Customizing Keyword Blocking URL Checking ............................................... 242
12.10.1 Domain Name or IP Address URL Checking .......................................... 242
12.10.2 Full Path URL Checking ......................................................................... 243
12.10.3 File Name URL Checking ........................................................................ 243
12.11 Content Filtering Cache .................................................................................. 243

**Chapter 13**
**Content Filtering Reports...................................................................................245**

13.1 Checking Content Filtering Activation .............................................................. 245
13.2 Viewing Content Filtering Reports .................................................................... 245
13.3 Web Site Submission ........................................................................................ 250

**Chapter 14**
**IPSec VPN....................................................................253**

14.1 IPSec VPN Overview .................................................... 253
    14.1.1 IKE SA Overview .................................................... 254
14.2 VPN Rules (IKE) .................................................... 255
14.3 IKE SA Setup .................................................... 257
    14.3.1 IKE SA Proposal .................................................... 257
14.4 Additional IPSec VPN Topics .................................................... 261
    14.4.1 SA Life Time .................................................... 262
    14.4.2 IPSec High Availability .................................................... 262
    14.4.3 Encryption and Authentication Algorithms .................................................... 263
14.5 VPN Rules (IKE) Gateway Policy Edit .................................................... 264
14.6 IPSec SA Overview .................................................... 270
    14.6.1 Local Network and Remote Network .................................................... 270
    14.6.2 Virtual Address Mapping .................................................... 271
    14.6.3 Active Protocol .................................................... 272
    14.6.4 Encapsulation .................................................... 272
    14.6.5 IPSec SA Proposal and Perfect Forward Secrecy .................................................... 273
14.7 VPN Rules (IKE) Network Policy Edit .................................................... 273
14.8 Network Policy Port Forwarding .................................................... 278
14.9 Network Policy Move .................................................... 280
14.10 IPSec SA Using Manual Keys .................................................... 281
    14.10.1 IPSec SA Proposal Using Manual Keys .................................................... 281
    14.10.2 Authentication and the Security Parameter Index (SPI) .................................................... 281
14.11 VPN Rules (Manual) .................................................... 281
14.12 VPN Rules (Manual) Edit .................................................... 283
14.13 VPN SA Monitor .................................................... 285
14.14 VPN Global Setting .................................................... 286
    14.14.1 Local and Remote IP Address Conflict Resolution .................................................... 286
14.15 Telecommuter VPN/IPSec Examples .................................................... 289
    14.15.1 Telecommuters Sharing One VPN Rule Example .................................................... 289
    14.15.2 Telecommuters Using Unique VPN Rules Example .................................................... 290
14.16 VPN and Remote Management .................................................... 291
14.17 Hub-and-spoke VPN .................................................... 292
    14.17.1 Hub-and-spoke VPN Example .................................................... 293
    14.17.2 Hub-and-spoke Example VPN Rule Addresses .................................................... 293
    14.17.3 Hub-and-spoke VPN Requirements and Suggestions .................................................... 294

**Chapter 15**
**Certificates ....................................................................295**

15.1 Certificates Overview .................................................... 295
    15.1.1 Advantages of Certificates .................................................... 296
15.2 Self-signed Certificates .................................................... 296

15.3 Verifying a Certificate ........ 296
    15.3.1 Checking the Fingerprint of a Certificate on Your Computer ........ 296
15.4 Configuration Summary ........ 297
15.5 My Certificates ........ 298
15.6 My Certificate Details ........ 300
15.7 My Certificate Export ........ 302
    15.7.1 Certificate File Export Formats ........ 302
15.8 My Certificate Import ........ 303
    15.8.1 Certificate File Formats ........ 303
15.9 My Certificate Create ........ 305
15.10 Trusted CAs ........ 310
15.11 Trusted CA Details ........ 312
15.12 Trusted CA Import ........ 314
15.13 Trusted Remote Hosts ........ 315
15.14 Trusted Remote Host Certificate Details ........ 316
15.15 Trusted Remote Hosts Import ........ 319
15.16 Directory Servers ........ 320
15.17 Directory Server Add or Edit ........ 321

**Chapter 16**
**Authentication Server........ 323**

16.1 Authentication Server Overview ........ 323
    16.1.1 Local User Database ........ 323
    16.1.2 RADIUS ........ 323
    16.1.3 Types of RADIUS Messages ........ 323
16.2 Local User Database ........ 324
16.3 RADIUS ........ 326

**Part IV: Advanced ........ 329**

**Chapter 17**
**Network Address Translation (NAT)........ 331**

17.1 NAT Overview ........ 331
    17.1.1 NAT Definitions ........ 331
    17.1.2 What NAT Does ........ 332
    17.1.3 How NAT Works ........ 332
    17.1.4 NAT Application ........ 333
    17.1.5 Port Restricted Cone NAT ........ 334
    17.1.6 NAT Mapping Types ........ 334
17.2 Using NAT ........ 335
    17.2.1 SUA (Single User Account) Versus NAT ........ 335

17.3 NAT Overview Screen ........ 336
17.4 NAT Address Mapping ........ 337
  17.4.1 What NAT Does ........ 337
  17.4.2 NAT Address Mapping Edit ........ 339
17.5 Port Forwarding ........ 340
  17.5.1 Default Server IP Address ........ 340
  17.5.2 Port Forwarding: Services and Port Numbers ........ 341
  17.5.3 Configuring Servers Behind Port Forwarding (Example) ........ 341
  17.5.4 Port Translation ........ 341
17.6 Port Forwarding Screen ........ 342
17.7 Port Triggering ........ 344

**Chapter 18**
**Static Route ........ 347**

18.1 IP Static Route ........ 347
18.2 IP Static Route ........ 348
  18.2.1 IP Static Route Edit ........ 349

**Chapter 19**
**Bandwidth Management ........ 351**

19.1 Bandwidth Management Overview ........ 351
19.2 Bandwidth Classes and Filters ........ 351
19.3 Proportional Bandwidth Allocation ........ 352
19.4 Application-based Bandwidth Management ........ 352
19.5 Subnet-based Bandwidth Management ........ 352
19.6 Application and Subnet-based Bandwidth Management ........ 352
19.7 Scheduler ........ 353
  19.7.1 Priority-based Scheduler ........ 353
  19.7.2 Fairness-based Scheduler ........ 353
  19.7.3 Maximize Bandwidth Usage ........ 353
  19.7.4 Reserving Bandwidth for Non-Bandwidth Class Traffic ........ 353
  19.7.5 Maximize Bandwidth Usage Example ........ 354
19.8 Bandwidth Borrowing ........ 355
  19.8.1 Bandwidth Borrowing Example ........ 355
19.9 Maximize Bandwidth Usage With Bandwidth Borrowing ........ 356
19.10 Over Allotment of Bandwidth ........ 356
19.11 Configuring Summary ........ 357
19.12 Configuring Class Setup ........ 358
  19.12.1 Bandwidth Manager Class Configuration ........ 359
  19.12.2 Bandwidth Management Statistics ........ 362
19.13 Bandwidth Manager Monitor ........ 363

**Chapter 20**
**DNS ........ 365**

20.1 DNS Overview ..... 365
20.2 DNS Server Address Assignment ..... 365
20.3 DNS Servers ..... 365
20.4 Address Record ..... 366
    20.4.1 DNS Wildcard ..... 366
20.5 Name Server Record ..... 366
    20.5.1 Private DNS Server ..... 366
20.6 System Screen ..... 367
    20.6.1 Adding an Address Record ..... 368
    20.6.2 Inserting a Name Server Record ..... 369
20.7 DNS Cache ..... 371
20.8 Configure DNS Cache ..... 371
20.9 Configuring DNS DHCP ..... 372
20.10 Dynamic DNS ..... 374
    20.10.1 DYNDNS Wildcard ..... 374
20.11 Configuring Dynamic DNS ..... 374

**Chapter 21**
**Remote Management..... 377**

21.1 Remote Management Overview ..... 377
    21.1.1 Remote Management Limitations ..... 378
    21.1.2 System Timeout ..... 378
21.2 WWW (HTTP and HTTPS) ..... 378
21.3 WWW Configuration ..... 379
21.4 HTTPS Example ..... 380
    21.4.1 Internet Explorer Warning Messages ..... 381
    21.4.2 Netscape Navigator Warning Messages ..... 381
    21.4.3 Avoiding the Browser Warning Messages ..... 382
    21.4.4 Login Screen ..... 383
21.5 SSH ..... 385
21.6 How SSH Works ..... 385
21.7 SSH Implementation on the ZyWALL ..... 386
    21.7.1 Requirements for Using SSH ..... 386
21.8 Configuring SSH ..... 386
21.9 Secure Telnet Using SSH Examples ..... 387
    21.9.1 Example 1: Microsoft Windows ..... 387
    21.9.2 Example 2: Linux ..... 388
21.10 Secure FTP Using SSH Example ..... 389
21.11 Telnet ..... 390
21.12 Configuring TELNET ..... 390
21.13 FTP ..... 391
21.14 SNMP ..... 392
    21.14.1 Supported MIBs ..... 393

21.14.2 SNMP Traps ........ 393
21.14.3 REMOTE MANAGEMENT: SNMP ........ 393
21.15 DNS ........ 395
21.16 Introducing Vantage CNM ........ 395
21.17 Configuring CNM ........ 396
21.17.1 Additional Configuration for Vantage CNM ........ 397

**Chapter 22**
**UPnP ........ 399**

22.1 Universal Plug and Play Overview ........ 399
22.1.1 How Do I Know If I'm Using UPnP? ........ 399
22.1.2 NAT Traversal ........ 399
22.1.3 Cautions with UPnP ........ 399
22.1.4 UPnP and ZyXEL ........ 400
22.2 Configuring UPnP ........ 400
22.3 Displaying UPnP Port Mapping ........ 401
22.4 Installing UPnP in Windows Example ........ 402
22.4.1 Installing UPnP in Windows Me ........ 403
22.4.2 Installing UPnP in Windows XP ........ 404
22.5 Using UPnP in Windows XP Example ........ 404
22.5.1 Auto-discover Your UPnP-enabled Network Device ........ 405
22.5.2 Web Configurator Easy Access ........ 406

**Chapter 23**
**Custom Application ........ 409**

23.1 Custom Applicaton ........ 409
23.2 Custom Applicaton Configuration ........ 409

**Chapter 24**
**ALG Screen ........ 411**

24.1 ALG Introduction ........ 411
24.1.1 ALG and NAT ........ 411
24.1.2 ALG and the Firewall ........ 411
24.2 FTP ........ 412
24.3 H.323 ........ 412
24.4 RTP ........ 412
24.4.1 H.323 ALG Details ........ 412
24.5 SIP ........ 413
24.5.1 STUN ........ 413
24.5.2 SIP ALG Details ........ 413
24.5.3 SIP Signaling Session Timeout ........ 414
24.5.4 SIP Audio Session Timeout ........ 414
24.6 ALG Screen ........ 414

**Part V: Logs and Maintenance ........................................................ 417**

**Chapter 25**
**Logs Screens ........................................................................................419**

25.1 Configuring View Log ........................................................................ 419
25.2 Log Description Example ................................................................... 420
  25.2.1 About the Certificate Not Trusted Log ........................................ 421
25.3 Configuring Log Settings ................................................................... 422
25.4 Configuring Reports ........................................................................... 425
  25.4.1 Viewing Web Site Hits ................................................................. 427
  25.4.2 Viewing Host IP Address ............................................................. 427
  25.4.3 Viewing Protocol/Port .................................................................. 428
  25.4.4 System Reports Specifications .................................................... 430
25.5 Log Descriptions ................................................................................ 430
25.6 Syslog Logs ....................................................................................... 445

**Chapter 26**
**Maintenance ........................................................................................447**

26.1 Maintenance Overview ........................................................................ 447
26.2 General Setup and System Name ...................................................... 447
  26.2.1 General Setup ............................................................................. 447
26.3 Configuring Password ........................................................................ 448
26.4 Time and Date .................................................................................... 449
26.5 Pre-defined NTP Time Server Pools ................................................... 452
  26.5.1 Resetting the Time ....................................................................... 452
  26.5.2 Time Server Synchronization ....................................................... 452
26.6 Introduction To Transparent Bridging ................................................. 453
26.7 Transparent Firewalls ......................................................................... 454
26.8 Configuring Device Mode (Router) ..................................................... 454
26.9 Configuring Device Mode (Bridge) ..................................................... 455
26.10 F/W Upload Screen .......................................................................... 457
26.11 Backup and Restore ......................................................................... 459
  26.11.1 Backup Configuration ................................................................ 460
  26.11.2 Restore Configuration ................................................................ 460
  26.11.3 Back to Factory Defaults ............................................................ 461
26.12 Restart Screen .................................................................................. 461
26.13 Diagnostics ....................................................................................... 462

**Part VI: SMT ........................................................................................ 465**

**Chapter 27**
**Introducing the SMT ........................................................................................ 467**

27.1 Introduction to the SMT .............................................................................. 467
27.2 Accessing the SMT via the Console Port .................................................... 467
27.2.1 Initial Screen .......................................................................................... 467
27.2.2 Entering the Password .......................................................................... 468
27.3 Navigating the SMT Interface ...................................................................... 468
27.3.1 Main Menu ............................................................................................. 469
27.3.2 SMT Menus Overview ........................................................................... 471
27.4 Changing the System Password ................................................................. 472
27.5 Resetting the ZyWALL ................................................................................ 473

**Chapter 28**
**SMT Menu 1 - General Setup ......................................................................... 475**

28.1 Introduction to General Setup ..................................................................... 475
28.2 Configuring General Setup .......................................................................... 475
28.2.1 Configuring Dynamic DNS ..................................................................... 476

**Chapter 29**
**WAN and Dial Backup Setup........................................................................... 481**

29.1 Introduction to WAN and Dial Backup Setup ............................................... 481
29.2 WAN Setup .................................................................................................. 481
29.3 Dial Backup ................................................................................................. 482
29.4 Configuring Dial Backup in Menu 2 ............................................................. 482
29.5 Advanced WAN Setup ................................................................................. 483
29.6 Remote Node Profile (Backup ISP) ............................................................. 485
29.7 Editing TCP/IP Options ................................................................................ 487
29.8 Editing Login Script ...................................................................................... 488
29.9 Remote Node Filter ...................................................................................... 489

**Chapter 30**
**LAN Setup......................................................................................................... 491**

30.1 Introduction to LAN Setup ........................................................................... 491
30.2 Accessing the LAN Menus ........................................................................... 491
30.3 LAN Port Filter Setup ................................................................................... 491
30.4 TCP/IP and DHCP Ethernet Setup Menu .................................................... 492
30.4.1 IP Alias Setup ........................................................................................ 495

**Chapter 31**
**Internet Access ................................................................................................ 497**

31.1 Introduction to Internet Access Setup .......................................................... 497
31.2 Ethernet Encapsulation ................................................................................ 497
31.3 Configuring the PPTP Client ........................................................................ 499

31.4 Configuring the PPPoE Client ........ 499
31.5 Basic Setup Complete ........ 500

**Chapter 32**
**DMZ Setup ........ 501**

32.1 Configuring DMZ Setup ........ 501
32.2 DMZ Port Filter Setup ........ 501
32.3 TCP/IP Setup ........ 502
32.3.1 IP Address ........ 502
32.3.2 IP Alias Setup ........ 503

**Chapter 33**
**Wireless Setup ........ 505**

33.1 TCP/IP Setup ........ 505
33.1.1 IP Address ........ 505
33.1.2 IP Alias Setup ........ 506

**Chapter 34**
**Remote Node Setup ........ 509**

34.1 Introduction to Remote Node Setup ........ 509
34.2 Remote Node Setup ........ 509
34.3 Remote Node Profile Setup ........ 509
34.3.1 Ethernet Encapsulation ........ 510
34.3.2 PPPoE Encapsulation ........ 511
34.3.3 PPTP Encapsulation ........ 513
34.4 Edit IP ........ 514
34.5 Remote Node Filter ........ 516
34.6 Traffic Redirect ........ 517

**Chapter 35**
**IP Static Route Setup ........ 519**

35.1 IP Static Route Setup ........ 519

**Chapter 36**
**Network Address Translation (NAT) ........ 521**

36.1 Using NAT ........ 521
36.1.1 SUA (Single User Account) Versus NAT ........ 521
36.1.2 Applying NAT ........ 521
36.2 NAT Setup ........ 523
36.2.1 Address Mapping Sets ........ 523
36.3 Configuring a Server behind NAT ........ 528
36.4 General NAT Examples ........ 530
36.4.1 Internet Access Only ........ 530

36.4.2 Example 2: Internet Access with a Default Server ............................................... 532
36.4.3 Example 3: Multiple Public IP Addresses With Inside Servers .............................. 532
36.4.4 Example 4: NAT Unfriendly Application Programs ............................................... 536
36.5 Trigger Port Forwarding ........................................................................................... 537
36.5.1 Two Points To Remember About Trigger Ports ................................................... 537

**Chapter 37**
**Introducing the ZyWALL Firewall.......................................................................... 539**

37.1 Using ZyWALL SMT Menus ...................................................................................... 539
37.1.1 Activating the Firewall ........................................................................................ 539

**Chapter 38**
**Filter Configuration................................................................................................ 541**

38.1 Introduction to Filters ............................................................................................... 541
38.1.1 The Filter Structure of the ZyWALL ...................................................................... 542
38.2 Configuring a Filter Set ............................................................................................ 544
38.2.1 Configuring a Filter Rule ..................................................................................... 546
38.2.2 Configuring a TCP/IP Filter Rule ......................................................................... 546
38.2.3 Configuring a Generic Filter Rule ........................................................................ 549
38.3 Example Filter ........................................................................................................... 550
38.4 Filter Types and NAT ................................................................................................ 552
38.5 Firewall Versus Filters ............................................................................................... 552
38.5.1 Packet Filtering: ................................................................................................... 552
38.5.2 Firewall ................................................................................................................ 553
38.6 Applying a Filter ....................................................................................................... 553
38.6.1 Applying LAN Filters ........................................................................................... 554
38.6.2 Applying DMZ Filters .......................................................................................... 554
38.6.3 Applying Remote Node Filters ............................................................................ 555

**Chapter 39**
**SNMP Configuration................................................................................................ 557**

39.1 SNMP Configuration ................................................................................................. 557
39.2 SNMP Traps ............................................................................................................. 558

**Chapter 40**
**System Information & Diagnosis.......................................................................... 559**

40.1 Introduction to System Status .................................................................................. 559
40.2 System Status ........................................................................................................... 559
40.3 System Information and Console Port Speed ........................................................... 561
40.3.1 System Information ............................................................................................. 561
40.3.2 Console Port Speed ............................................................................................ 562
40.4 Log and Trace ........................................................................................................... 562
40.4.1 Viewing Error Log ............................................................................................... 562

40.4.2 Syslog Logging ........................................ 563
40.4.3 Call-Triggering Packet ........................................ 566
40.5 Diagnostic ........................................ 567
40.5.1 WAN DHCP ........................................ 568

**Chapter 41**
**Firmware and Configuration File Maintenance ........................................ 571**

41.1 Introduction ........................................ 571
41.2 Filename Conventions ........................................ 571
41.3 Backup Configuration ........................................ 572
41.3.1 Backup Configuration ........................................ 572
41.3.2 Using the FTP Command from the Command Line ........................................ 573
41.3.3 Example of FTP Commands from the Command Line ........................................ 574
41.3.4 GUI-based FTP Clients ........................................ 574
41.3.5 File Maintenance Over WAN ........................................ 574
41.3.6 Backup Configuration Using TFTP ........................................ 575
41.3.7 TFTP Command Example ........................................ 575
41.3.8 GUI-based TFTP Clients ........................................ 575
41.3.9 Backup Via Console Port ........................................ 576
41.4 Restore Configuration ........................................ 577
41.4.1 Restore Using FTP ........................................ 577
41.4.2 Restore Using FTP Session Example ........................................ 578
41.4.3 Restore Via Console Port ........................................ 579
41.5 Uploading Firmware and Configuration Files ........................................ 579
41.5.1 Firmware File Upload ........................................ 580
41.5.2 Configuration File Upload ........................................ 580
41.5.3 FTP File Upload Command from the DOS Prompt Example ........................................ 581
41.5.4 FTP Session Example of Firmware File Upload ........................................ 582
41.5.5 TFTP File Upload ........................................ 582
41.5.6 TFTP Upload Command Example ........................................ 583
41.5.7 Uploading Via Console Port ........................................ 583
41.5.8 Uploading Firmware File Via Console Port ........................................ 583
41.5.9 Example Xmodem Firmware Upload Using HyperTerminal ........................................ 583
41.5.10 Uploading Configuration File Via Console Port ........................................ 584
41.5.11 Example Xmodem Configuration Upload Using HyperTerminal ........................................ 585

**Chapter 42**
**System Maintenance Menus 8 to 10 ........................................ 587**

42.1 Command Interpreter Mode ........................................ 587
42.1.1 Command Syntax ........................................ 588
42.1.2 Command Usage ........................................ 588
42.2 Call Control Support ........................................ 589
42.2.1 Budget Management ........................................ 589

42.2.2 Call History .......... 590
42.3 Time and Date Setting .......... 591

**Chapter 43**
**Remote Management .......... 595**

43.1 Remote Management .......... 595
43.1.1 Remote Management Limitations .......... 597

**Chapter 44**
**Call Scheduling .......... 599**

44.1 Introduction to Call Scheduling .......... 599

**Part VII: Troubleshooting and Specifications .......... 603**

**Chapter 45**
**Troubleshooting .......... 605**

45.1 Power, Hardware Connections, and LEDs .......... 605
45.2 ZyWALL Access and Login .......... 606
45.3 Internet Access .......... 608
45.4 Wireless Router/AP Troubleshooting .......... 610
45.5 UPnP .......... 610

**Chapter 46**
**Product Specifications .......... 613**

46.1 General ZyWALL Specifications .......... 613
46.2 Cable Pin Assignments .......... 615
46.3 Wall-mounting Instructions .......... 617

**Part VIII: Appendices and Index .......... 619**

Appendix A Setting up Your Computer’s IP Address .......... 621

Appendix B Pop-up Windows, JavaScripts and Java Permissions .......... 637

Appendix C IP Addresses and Subnetting .......... 645

Appendix D Common Services .......... 653

Appendix E Importing Certificates .......... 657

Appendix F Legal Information .......... 669

Appendix G Customer Support .......... 673

**Index..................................................................................................................... 679**

# List of Figures

Figure 1 Secure Internet Access via Cable, DSL or Wireless Modem ..... 48
Figure 2 VPN Application ..... 48
Figure 3 Front Panel ..... 49
Figure 4 Change Password Screen ..... 52
Figure 5 Replace Certificate Screen ..... 52
Figure 6 Example Xmodem Upload ..... 53
Figure 7 HOME Screen ..... 54
Figure 8 Web Configurator HOME Screen in Router Mode ..... 55
Figure 9 Web Configurator HOME Screen in Bridge Mode ..... 58
Figure 10 HOME > Show Statistics ..... 64
Figure 11 HOME > DHCP Table ..... 65
Figure 12 HOME > VPN Status ..... 66
Figure 13 Home > Bandwidth Monitor ..... 67
Figure 14 Wizard Setup Welcome ..... 69
Figure 15 ISP Parameters: Ethernet Encapsulation ..... 70
Figure 16 ISP Parameters: PPPoE Encapsulation ..... 72
Figure 17 ISP Parameters: PPTP Encapsulation ..... 74
Figure 18 Internet Access Wizard: Second Screen ..... 75
Figure 19 Internet Access Setup Complete ..... 76
Figure 20 Internet Access Wizard: Registration ..... 77
Figure 21 Internet Access Wizard: Registration in Progress ..... 78
Figure 22 Internet Access Wizard: Status ..... 78
Figure 23 Internet Access Wizard: Registration Failed ..... 78
Figure 24 Internet Access Wizard: Registered Device ..... 79
Figure 25 Internet Access Wizard: Activated Services ..... 79
Figure 26 VPN Wizard: Gateway Setting ..... 80
Figure 27 VPN Wizard: Network Setting ..... 81
Figure 28 VPN Wizard: IKE Tunnel Setting ..... 82
Figure 29 VPN Wizard: IPSec Setting ..... 84
Figure 30 VPN Wizard: VPN Status ..... 85
Figure 31 VPN Wizard Setup Complete ..... 87
Figure 32 Firewall Rule for VPN ..... 90
Figure 33 SECURITY > VPN > VPN Rules (IKE) ..... 90
Figure 34 SECURITY > VPN > VPN Rules (IKE)> Add Gateway Policy ..... 91
Figure 35 SECURITY > VPN > VPN Rules (IKE): With Gateway Policy Example ..... 92
Figure 36 SECURITY > VPN > VPN Rules (IKE)> Add Network Policy ..... 93
Figure 37 SECURITY > FIREWALL > Rule Summary ..... 94
Figure 38 SECURITY > FIREWALL > Rule Summary > Edit: Allow ..... 95

Figure 39 SECURITY > FIREWALL > Rule Summary: Allow .......... 96
Figure 40 SECURITY > FIREWALL > Default Rule: Block From VPN To LAN .......... 96
Figure 41 Tutorial Example: Using NAT with Static Public IP Addresses .......... 97
Figure 42 Tutorial Example: WAN Connection with a Static Public IP Address .......... 98
Figure 43 Tutorial Example: WAN Screen .......... 99
Figure 44 Tutorial Example: DNS > System .......... 99
Figure 45 Tutorial Example: DNS > System Edit-1 .......... 100
Figure 46 Tutorial Example: DNS > System Edit-2 .......... 100
Figure 47 Tutorial Example: DNS > System: Done .......... 101
Figure 48 Tutorial Example: Status .......... 101
Figure 49 Tutorial Example: Mapping Multiple Public IP Addresses to Inside Servers .......... 102
Figure 50 Tutorial Example: NAT > NAT Overview .......... 103
Figure 51 Tutorial Example: NAT > Address Mapping .......... 103
Figure 52 Tutorial Example: NAT Address Mapping Edit: One-to-One (1) .......... 104
Figure 53 Tutorial Example: NAT Address Mapping Edit: One-to-One (2) .......... 104
Figure 54 Tutorial Example: NAT Address Mapping Edit: Many-to-One .......... 104
Figure 55 Tutorial Example: NAT Address Mapping Done .......... 105
Figure 56 Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer .......... 106
Figure 57 Tutorial Example: NAT Address Mapping Edit: Server .......... 106
Figure 58 Tutorial Example: NAT Port Forwarding .......... 107
Figure 59 Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer .......... 107
Figure 60 Tutorial Example: Firewall Default Rule .......... 108
Figure 61 Tutorial Example: Firewall Rule: WAN to LAN .......... 108
Figure 62 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Web Server .......... 109
Figure 63 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Web Server .......... 110
Figure 64 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Mail Server .......... 111
Figure 65 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Mail Server .......... 111
Figure 66 Tutorial Example: Firewall Rule: WAN to LAN Address Edit for FTP Server .......... 112
Figure 67 Tutorial Example: Firewall Rule: WAN to LAN Service Edit for FTP Server .......... 113
Figure 68 Tutorial Example: Firewall Rule Summary .......... 113
Figure 69 Tutorial Example: NAT Address Mapping Done: Game Playing .......... 115
Figure 70 Tutorial Example: Bandwidth Management .......... 116
Figure 71 Tutorial Example: Bandwidth Management Summary .......... 117
Figure 72 Tutorial Example: Bandwidth Management Class Setup .......... 117
Figure 73 Tutorial Example: Bandwidth Management Class Setup: VoIP .......... 118
Figure 74 Tutorial Example: Bandwidth Management Class Setup: FTP .......... 118
Figure 75 Tutorial Example: Bandwidth Management Class Setup: WWW .......... 119
Figure 76 Tutorial Example: Bandwidth Management Class Setup Done .......... 119
Figure 77 Tutorial Example: Bandwidth Management Monitor .......... 120
Figure 78 SECURITY > CONTENT FILTER > General .......... 121
Figure 79 SECURITY > CONTENT FILTER > Policy .......... 122
Figure 80 SECURITY > CONTENT FILTER > Policy > External Database (Default) .......... 122
Figure 81 HOME > DHCP Table .......... 123

Figure 82 SECURITY > CONTENT FILTER > Policy ..... 123
Figure 83 SECURITY > CONTENT FILTER > Policy > Insert ..... 124
Figure 84 SECURITY > CONTENT FILTER > Policy ..... 124
Figure 85 SECURITY > CONTENT FILTER > Policy > Schedule (Bob) ..... 125
Figure 86 SECURITY > CONTENT FILTER > Policy ..... 125
Figure 87 SECURITY > CONTENT FILTER > Policy > External Database (Bob) ..... 126
Figure 88 REGISTRATION ..... 128
Figure 89 REGISTRATION: Registered Device ..... 129
Figure 90 REGISTRATION > Service ..... 130
Figure 91 LAN and WAN ..... 133
Figure 92 NETWORK > LAN ..... 137
Figure 93 NETWORK > LAN > Static DHCP ..... 139
Figure 94 Physical Network & Partitioned Logical Networks ..... 140
Figure 95 NETWORK > LAN > IP Alias ..... 141
Figure 96 NETWORK > LAN > Port Roles ..... 142
Figure 97 Port Roles Change Complete ..... 143
Figure 98 Bridge Loop: Bridge Connected to Wired LAN ..... 145
Figure 99 NETWORK > Bridge ..... 148
Figure 100 NETWORK > Bridge > Port Roles ..... 150
Figure 101 Port Roles Change Complete ..... 150
Figure 102 NETWORK > WAN Route ..... 152
Figure 103 NETWORK > WAN > WAN (Ethernet Encapsulation) ..... 155
Figure 104 NETWORK > WAN > WAN (PPPoE Encapsulation) ..... 158
Figure 105 NETWORK > WAN > WAN (PPTP Encapsulation) ..... 161
Figure 106 Traffic Redirect WAN Setup ..... 164
Figure 107 Traffic Redirect LAN Setup ..... 164
Figure 108 NETWORK > WAN > Traffic Redirect ..... 164
Figure 109 NETWORK > WAN > Dial Backup ..... 166
Figure 110 NETWORK > WAN > Dial Backup > Edit ..... 169
Figure 111 NETWORK > DMZ ..... 172
Figure 112 NETWORK > DMZ > Static DHCP ..... 174
Figure 113 NETWORK > DMZ > IP Alias ..... 176
Figure 114 DMZ Public Address Example ..... 177
Figure 115 DMZ Private and Public Address Example ..... 178
Figure 116 NETWORK > DMZ > Port Roles ..... 179
Figure 117 NETWORK > WLAN ..... 182
Figure 118 NETWORK > WLAN > Static DHCP ..... 184
Figure 119 NETWORK > WLAN > IP Alias ..... 186
Figure 120 WLAN Port Role Example ..... 187
Figure 121 NETWORK > WLAN > Port Roles ..... 188
Figure 122 NETWORK > WLAN > Port Roles: Change Complete ..... 188
Figure 123 Default Firewall Action ..... 191
Figure 124 SECURITY > FIREWALL > Default Rule (Router Mode) ..... 192

Figure 125 Default Block Traffic From WAN to DMZ Example ........................................................ 193
Figure 126 From LAN to VPN Example ........................................................................................ 195
Figure 127 Block DMZ to VPN Traffic by Default Example ........................................................... 196
Figure 128 From VPN to LAN Example ........................................................................................ 197
Figure 129 Block VPN to LAN Traffic by Default Example ............................................................ 197
Figure 130 From VPN to VPN Example ........................................................................................ 198
Figure 131 Block VPN to VPN Traffic by Default Example ........................................................... 199
Figure 132 Blocking All LAN to WAN IRC Traffic Example ............................................................ 200
Figure 133 Limited LAN to WAN IRC Traffic Example ................................................................... 201
Figure 134 Using IP Alias to Solve the Triangle Route Problem ................................................... 202
Figure 135 SECURITY > FIREWALL > Default Rule (Router Mode) ............................................. 203
Figure 136 SECURITY > FIREWALL > Default Rule (Bridge Mode) .............................................. 205
Figure 137 SECURITY > FIREWALL > Rule Summary ................................................................. 207
Figure 138 SECURITY > FIREWALL > Rule Summary > Edit ....................................................... 209
Figure 139 SECURITY > FIREWALL > Anti-Probing .....................................................................211
Figure 140 Three-Way Handshake .............................................................................................. 212
Figure 141 SECURITY > FIREWALL > Threshold ........................................................................ 213
Figure 142 SECURITY > FIREWALL > Service ............................................................................ 215
Figure 143 Firewall Edit Custom Service ..................................................................................... 216
Figure 144 My Service Firewall Rule Example: Service ............................................................... 217
Figure 145 My Service Firewall Rule Example: Edit Custom Service ........................................... 217
Figure 146 My Service Firewall Rule Example: Rule Summary .................................................... 218
Figure 147 My Service Firewall Rule Example: Rule Edit: Source and Destination Addresses .......... 218
Figure 148 My Service Firewall Rule Example: Edit Rule: Service Configuration ............................... 220
Figure 149 My Service Firewall Rule Example: Rule Summary: Completed ...................................... 221
Figure 150 Content Filtering Lookup Procedure ........................................................................... 224
Figure 151 SECURITY > CONTENT FILTER > General ................................................................ 225
Figure 152 SECURITY > CONTENT FILTER > Policy ................................................................... 228
Figure 153 SECURITY > CONTENT FILTER > Policy > General .................................................. 229
Figure 154 SECURITY > CONTENT FILTER > Policy > External Database .................................. 231
Figure 155 SECURITY > CONTENT FILTER > Policy > Customization ......................................... 238
Figure 156 SECURITY > CONTENT FILTER > Policy > Schedule ................................................. 240
Figure 157 SECURITY > CONTENT FILTER > Object .................................................................. 241
Figure 158 SECURITY > CONTENT FILTER > Cache .................................................................. 244
Figure 159 myZyXEL.com: Login .................................................................................................. 246
Figure 160 myZyXEL.com: Welcome ............................................................................................ 246
Figure 161 myZyXEL.com: Service Management ......................................................................... 247
Figure 162 Blue Coat: Login ......................................................................................................... 247
Figure 163 Content Filtering Reports Main Screen ....................................................................... 248
Figure 164 Blue Coat: Report Home ............................................................................................. 248
Figure 165 Global Report Screen Example .................................................................................. 249
Figure 166 Requested URLs Example .......................................................................................... 250
Figure 167 Web Page Review Process Screen ............................................................................ 251

Figure 168 VPN: Example ........ 253
Figure 169 VPN: IKE SA and IPSec SA ........ 254
Figure 170 Gateway and Network Policies ........ 255
Figure 171 IPSec Fields Summary ........ 255
Figure 172 SECURITY > VPN > VPN Rules (IKE) ........ 256
Figure 173 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal ........ 257
Figure 174 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange ........ 258
Figure 175 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication ........ 258
Figure 176 VPN/NAT Example ........ 261
Figure 177 IPSec High Availability ........ 263
Figure 178 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy ........ 265
Figure 179 Virtual Mapping of Local and Remote Network IP Addresses ........ 271
Figure 180 VPN: Transport and Tunnel Mode Encapsulation ........ 272
Figure 181 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy ........ 274
Figure 182 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding ........ 279
Figure 183 SECURITY > VPN > VPN Rules (IKE) > Move Network Policy ........ 280
Figure 184 SECURITY > VPN > VPN Rules (Manual) ........ 282
Figure 185 SECURITY > VPN > VPN Rules (Manual) > Edit ........ 283
Figure 186 SECURITY > VPN > SA Monitor ........ 286
Figure 187 Overlap in a Dynamic VPN Rule ........ 287
Figure 188 Overlap in IP Alias and VPN Remote Networks ........ 287
Figure 189 SECURITY > VPN > Global Setting ........ 288
Figure 190 Telecommuters Sharing One VPN Rule Example ........ 289
Figure 191 Telecommuters Using Unique VPN Rules Example ........ 290
Figure 192 VPN for Remote Management Example ........ 292
Figure 193 VPN Topologies ........ 292
Figure 194 Hub-and-spoke VPN Example ........ 293
Figure 195 Certificates on Your Computer ........ 296
Figure 196 Certificate Details ........ 297
Figure 197 Certificate Configuration Overview ........ 297
Figure 198 SECURITY > CERTIFICATES > My Certificates ........ 298
Figure 199 SECURITY > CERTIFICATES > My Certificates > Details ........ 300
Figure 200 SECURITY > CERTIFICATES > My Certificates > Export ........ 302
Figure 201 SECURITY > CERTIFICATES > My Certificates > Import ........ 304
Figure 202 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12 ........ 305
Figure 203 SECURITY > CERTIFICATES > My Certificates > Create (Basic) ........ 306
Figure 204 SECURITY > CERTIFICATES > My Certificates > Create (Advanced) ........ 307
Figure 205 SECURITY > CERTIFICATES > Trusted CAs ........ 311
Figure 206 SECURITY > CERTIFICATES > Trusted CAs > Details ........ 312
Figure 207 SECURITY > CERTIFICATES > Trusted CAs > Import ........ 315
Figure 208 SECURITY > CERTIFICATES > Trusted Remote Hosts ........ 315
Figure 209 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details ........ 317
Figure 210 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import ........ 319

Figure 211 SECURITY > CERTIFICATES > Directory Servers ........................................................ 320
Figure 212 SECURITY > CERTIFICATES > Directory Server > Add ................................................ 321
Figure 213 SECURITY > AUTH SERVER > Local User Database .................................................... 325
Figure 214 SECURITY > AUTH SERVER > RADIUS ......................................................................... 326
Figure 215 How NAT Works ........................................................................................................... 333
Figure 216 NAT Application With IP Alias ..................................................................................... 333
Figure 217 Port Restricted Cone NAT Example ............................................................................ 334
Figure 218 ADVANCED > NAT > NAT Overview ............................................................................ 336
Figure 219 ADVANCED > NAT > Address Mapping ....................................................................... 338
Figure 220 ADVANCED > NAT > Address Mapping > Edit ............................................................ 339
Figure 221 Multiple Servers Behind NAT Example ........................................................................ 341
Figure 222 Port Translation Example ............................................................................................. 342
Figure 223 ADVANCED > NAT > Port Forwarding ......................................................................... 343
Figure 224 Trigger Port Forwarding Process: Example ................................................................ 344
Figure 225 ADVANCED > NAT > Port Triggering .......................................................................... 345
Figure 226 Example of Static Routing Topology ........................................................................... 347
Figure 227 ADVANCED > STATIC ROUTE > IP Static Route ........................................................ 348
Figure 228 ADVANCED > STATIC ROUTE > IP Static Route > Edit ............................................. 349
Figure 229 Subnet-based Bandwidth Management Example ........................................................ 352
Figure 230 ADVANCED > BW MGMT > Summary ......................................................................... 357
Figure 231 ADVANCED > BW MGMT > Class Setup ..................................................................... 358
Figure 232 ADVANCED > BW MGMT > Class Setup > Add Sub-Class .......................................... 360
Figure 233 ADVANCED > BW MGMT > Class Setup > Statistics ................................................... 362
Figure 234 ADVANCED > BW MGMT > Monitor ............................................................................ 363
Figure 235 Private DNS Server Example ...................................................................................... 367
Figure 236 ADVANCED > DNS > System DNS .............................................................................. 367
Figure 237 ADVANCED > DNS > Add (Address Record) ............................................................... 369
Figure 238 ADVANCED > DNS > Insert (Name Server Record) ..................................................... 370
Figure 239 ADVANCED > DNS > Cache ........................................................................................ 371
Figure 240 ADVANCED > DNS > DHCP ......................................................................................... 373
Figure 241 ADVANCED > DNS > DDNS ......................................................................................... 375
Figure 242 Secure and Insecure Remote Management From the WAN ........................................ 377
Figure 243 HTTPS Implementation ................................................................................................ 379
Figure 244 ADVANCED > REMOTE MGMT > WWW ..................................................................... 379
Figure 245 Security Alert Dialog Box (Internet Explorer) ............................................................... 381
Figure 246 Security Certificate 1 (Netscape) ................................................................................. 382
Figure 247 Security Certificate 2 (Netscape) ................................................................................. 382
Figure 248 Example: Lock Denoting a Secure Connection ........................................................... 383
Figure 249 Replace Certificate ....................................................................................................... 384
Figure 250 Device-specific Certificate ........................................................................................... 384
Figure 251 Common ZyWALL Certificate ...................................................................................... 384
Figure 252 SSH Communication Over the WAN Example ............................................................ 385
Figure 253 How SSH Works .......................................................................................................... 385

Figure 254 ADVANCED > REMOTE MGMT > SSH ............ 387
Figure 255 SSH Example 1: Store Host Key ............ 388
Figure 256 SSH Example 2: Test ............ 388
Figure 257 SSH Example 2: Log in ............ 389
Figure 258 Secure FTP: Firmware Upload Example ............ 389
Figure 259 ADVANCED > REMOTE MGMT > TELNET ............ 390
Figure 260 ADVANCED > REMOTE MGMT > FTP ............ 391
Figure 261 SNMP Management Model ............ 392
Figure 262 ADVANCED > REMOTE MGMT > SNMP ............ 394
Figure 263 ADVANCED > REMOTE MGMT > DNS ............ 395
Figure 264 ADVANCED > REMOTE MGMT > CNM ............ 396
Figure 265 ADVANCED > UPnP ............ 400
Figure 266 ADVANCED > UPnP > Ports ............ 401
Figure 267 ADVANCED > Custom APP ............ 410
Figure 268 H.323 ALG Example ............ 412
Figure 269 SIP ALG Example ............ 414
Figure 270 ADVANCED > ALG ............ 415
Figure 271 LOGS > View Log ............ 419
Figure 272 myZyXEL.com: Download Center ............ 421
Figure 273 myZyXEL.com: Certificate Download ............ 422
Figure 274 LOGS > Log Settings ............ 423
Figure 275 LOGS > Reports ............ 426
Figure 276 LOGS > Reports: Web Site Hits Example ............ 427
Figure 277 LOGS > Reports: Host IP Address Example ............ 428
Figure 278 LOGS > Reports: Protocol/Port Example ............ 429
Figure 279 MAINTENANCE > General Setup ............ 448
Figure 280 MAINTENANCE > Password ............ 449
Figure 281 MAINTENANCE > Time and Date ............ 450
Figure 282 Synchronization in Process ............ 452
Figure 283 Synchronization is Successful ............ 453
Figure 284 Synchronization Fail ............ 453
Figure 285 MAINTENANCE > Device Mode (Router Mode) ............ 455
Figure 286 MAINTENANCE > Device Mode (Bridge Mode) ............ 456
Figure 287 MAINTENANCE > Firmware Upload ............ 457
Figure 288 Firmware Upload In Process ............ 458
Figure 289 Network Temporarily Disconnected ............ 458
Figure 290 Firmware Upload Error ............ 459
Figure 291 MAINTENANCE > Backup and Restore ............ 459
Figure 292 Configuration Upload Successful ............ 460
Figure 293 Network Temporarily Disconnected ............ 460
Figure 294 Configuration Upload Error ............ 461
Figure 295 Reset Warning Message ............ 461
Figure 296 MAINTENANCE > Restart ............ 462

Figure 297 MAINTENANCE > Diagnostics ............ 463
Figure 298 Initial Screen ............ 468
Figure 299 Password Screen ............ 468
Figure 300 Main Menu (Router Mode) ............ 469
Figure 301 Main Menu (Bridge Mode) ............ 470
Figure 302 Menu 23: System Password ............ 472
Figure 303 Menu 1: General Setup (Router Mode) ............ 475
Figure 304 Menu 1: General Setup (Bridge Mode) ............ 476
Figure 305 Menu 1.1: Configure Dynamic DNS ............ 477
Figure 306 Menu 1.1.1: DDNS Host Summary ............ 478
Figure 307 Menu 1.1.1: DDNS Edit Host ............ 479
Figure 308 MAC Address Cloning in WAN Setup ............ 481
Figure 309 Menu 2: Dial Backup Setup ............ 483
Figure 310 Menu 2.1: Advanced WAN Setup ............ 484
Figure 311 Menu 11.2: Remote Node Profile (Backup ISP) ............ 485
Figure 312 Menu 11.2.2: Remote Node Network Layer Options ............ 487
Figure 313 Menu 11.2.3: Remote Node Script ............ 489
Figure 314 Menu 11.2.4: Remote Node Filter ............ 490
Figure 315 Menu 3: LAN Setup ............ 491
Figure 316 Menu 3.1: LAN Port Filter Setup ............ 492
Figure 317 Menu 3: TCP/IP and DHCP Setup ............ 492
Figure 318 Menu 3.2: TCP/IP and DHCP Ethernet Setup ............ 493
Figure 319 Menu 3.2.1: IP Alias Setup ............ 495
Figure 320 Menu 4: Internet Access Setup (Ethernet) ............ 497
Figure 321 Internet Access Setup (PPTP) ............ 499
Figure 322 Internet Access Setup (PPPoE) ............ 500
Figure 323 Menu 5: DMZ Setup ............ 501
Figure 324 Menu 5.1: DMZ Port Filter Setup ............ 501
Figure 325 Menu 5: DMZ Setup ............ 502
Figure 326 Menu 5.2: TCP/IP and DHCP Ethernet Setup ............ 502
Figure 327 Menu 5.2.1: IP Alias Setup ............ 503
Figure 328 Menu 7: WLAN Setup ............ 505
Figure 329 Menu 7.2: TCP/IP and DHCP Ethernet Setup ............ 506
Figure 330 Menu 7.2.1: IP Alias Setup ............ 507
Figure 331 Menu 11: Remote Node Setup ............ 509
Figure 332 Menu 11.1: Remote Node Profile for Ethernet Encapsulation ............ 510
Figure 333 Menu 11.1: Remote Node Profile for PPPoE Encapsulation ............ 512
Figure 334 Menu 11.1: Remote Node Profile for PPTP Encapsulation ............ 514
Figure 335 Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation ............ 515
Figure 336 Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation) ............ 516
Figure 337 Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation) ............ 517
Figure 338 Menu 11.1.5: Traffic Redirect Setup ............ 517
Figure 339 Menu 12: IP Static Route Setup ............ 519

Figure 340 Menu 12. 1: Edit IP Static Route ........................................................................... 520
Figure 341 Menu 4: Applying NAT for Internet Access ............................................................ 522
Figure 342 Menu 11.1.2: Applying NAT to the Remote Node ................................................... 522
Figure 343 Menu 15: NAT Setup ................................................................................................ 523
Figure 344 Menu 15.1: Address Mapping Sets ......................................................................... 524
Figure 345 Menu 15.1.255: SUA Address Mapping Rules ........................................................ 524
Figure 346 Menu 15.1.1: First Set ............................................................................................. 526
Figure 347 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set ........................................ 527
Figure 348 Menu 15.2: NAT Server Sets ................................................................................... 528
Figure 349 15.2.1: NAT Server Configuration ........................................................................... 529
Figure 350 Menu 15.2: NAT Server Setup ................................................................................ 530
Figure 351 Server Behind NAT Example ................................................................................... 530
Figure 352 NAT Example 1 ........................................................................................................ 531
Figure 353 Menu 4: Internet Access & NAT Example .............................................................. 531
Figure 354 NAT Example 2 ........................................................................................................ 532
Figure 355 Menu 15.2: Specifying an Inside Server ................................................................. 532
Figure 356 NAT Example 3 ........................................................................................................ 533
Figure 357 Example 3: Menu 11.1.2 ......................................................................................... 534
Figure 358 Example 3: Menu 15.1.1.1 ...................................................................................... 534
Figure 359 Example 3: Final Menu 15.1.1 ................................................................................ 535
Figure 360 Example 3: Menu 15.2. ........................................................................................... 535
Figure 361 NAT Example 4 ........................................................................................................ 536
Figure 362 Example 4: Menu 15.1.1.1: Address Mapping Rule ............................................... 536
Figure 363 Example 4: Menu 15.1.1: Address Mapping Rules ................................................ 537
Figure 364 Menu 15.3.1: Trigger Port Setup ............................................................................ 538
Figure 365 Menu 21: Filter and Firewall Setup ......................................................................... 539
Figure 366 Menu 21.2: Firewall Setup ...................................................................................... 540
Figure 367 Outgoing Packet Filtering Process ......................................................................... 541
Figure 368 Filter Rule Process ................................................................................................. 543
Figure 369 Menu 21: Filter and Firewall Setup ......................................................................... 544
Figure 370 Menu 21.1: Filter Set Configuration ........................................................................ 544
Figure 371 Menu 21.1.1: Filter Rules Summary ....................................................................... 545
Figure 372 Menu 21.1.1.1: TCP/IP Filter Rule ......................................................................... 546
Figure 373 Executing an IP Filter ............................................................................................. 548
Figure 374 Menu 21.1.1.1: Generic Filter Rule ......................................................................... 549
Figure 375 Telnet Filter Example .............................................................................................. 550
Figure 376 Example Filter: Menu 21.1.3.1 ............................................................................... 551
Figure 377 Example Filter Rules Summary: Menu 21.1.3 ....................................................... 551
Figure 378 Protocol and Device Filter Sets .............................................................................. 552
Figure 379 Filtering LAN Traffic ................................................................................................ 554
Figure 380 Filtering DMZ Traffic ............................................................................................... 554
Figure 381 Filtering Remote Node Traffic ................................................................................. 555
Figure 382 Menu 22: SNMP Configuration ............................................................................... 557

Figure 383 Menu 24: System Maintenance .......... 559
Figure 384 Menu 24.1: System Maintenance: Status .......... 560
Figure 385 Menu 24.2: System Information and Console Port Speed .......... 561
Figure 386 Menu 24.2.1: System Maintenance: Information .......... 561
Figure 387 Menu 24.2.2: System Maintenance: Change Console Port Speed .......... 562
Figure 388 Menu 24.3: System Maintenance: Log and Trace .......... 563
Figure 389 Examples of Error and Information Messages .......... 563
Figure 390 Menu 24.3.2: System Maintenance: Syslog Logging .......... 563
Figure 391 Call-Triggering Packet Example .......... 567
Figure 392 Menu 24.4: System Maintenance: Diagnostic .......... 568
Figure 393 WAN & LAN DHCP .......... 568
Figure 394 Telnet into Menu 24.5 .......... 573
Figure 395 FTP Session Example .......... 574
Figure 396 System Maintenance: Backup Configuration .......... 576
Figure 397 System Maintenance: Starting Xmodem Download Screen .......... 576
Figure 398 Backup Configuration Example .......... 576
Figure 399 Successful Backup Confirmation Screen .......... 577
Figure 400 Telnet into Menu 24.6 .......... 578
Figure 401 Restore Using FTP Session Example .......... 578
Figure 402 System Maintenance: Restore Configuration .......... 579
Figure 403 System Maintenance: Starting Xmodem Download Screen .......... 579
Figure 404 Restore Configuration Example .......... 579
Figure 405 Successful Restoration Confirmation Screen .......... 579
Figure 406 Telnet Into Menu 24.7.1: Upload System Firmware .......... 580
Figure 407 Telnet Into Menu 24.7.2: System Maintenance .......... 581
Figure 408 FTP Session Example of Firmware File Upload .......... 582
Figure 409 Menu 24.7.1 As Seen Using the Console Port .......... 583
Figure 410 Example Xmodem Upload .......... 584
Figure 411 Menu 24.7.2 As Seen Using the Console Port .......... 584
Figure 412 Example Xmodem Upload .......... 585
Figure 413 Command Mode in Menu 24 .......... 587
Figure 414 Valid Commands .......... 588
Figure 415 Call Control .......... 589
Figure 416 Budget Management .......... 589
Figure 417 Call History .......... 590
Figure 418 Menu 24: System Maintenance .......... 591
Figure 419 Menu 24.10 System Maintenance: Time and Date Setting .......... 592
Figure 420 Menu 24.11 – Remote Management Control .......... 596
Figure 421 Schedule Setup .......... 599
Figure 422 Schedule Set Setup .......... 600
Figure 423 Applying Schedule Set(s) to a Remote Node (PPPoE) .......... 601
Figure 424 Applying Schedule Set(s) to a Remote Node (PPTP) .......... 602
Figure 425 Console/Dial Backup Cable DB-9 End Pin Layout .......... 616

Figure 426 Wall-mounting Example .......... 618
Figure 427 Masonry Plug and M4 Tap Screw .......... 618
Figure 428 WIndows 95/98/Me: Network: Configuration .......... 622
Figure 429 Windows 95/98/Me: TCP/IP Properties: IP Address .......... 623
Figure 430 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .......... 624
Figure 431 Windows XP: Start Menu .......... 625
Figure 432 Windows XP: Control Panel .......... 625
Figure 433 Windows XP: Control Panel: Network Connections: Properties .......... 626
Figure 434 Windows XP: Local Area Connection Properties .......... 626
Figure 435 Windows XP: Internet Protocol (TCP/IP) Properties .......... 627
Figure 436 Windows XP: Advanced TCP/IP Properties .......... 628
Figure 437 Windows XP: Internet Protocol (TCP/IP) Properties .......... 629
Figure 438 Macintosh OS 8/9: Apple Menu .......... 630
Figure 439 Macintosh OS 8/9: TCP/IP .......... 630
Figure 440 Macintosh OS X: Apple Menu .......... 631
Figure 441 Macintosh OS X: Network .......... 632
Figure 442 Red Hat 9.0: KDE: Network Configuration: Devices .......... 633
Figure 443 Red Hat 9.0: KDE: Ethernet Device: General .......... 633
Figure 444 Red Hat 9.0: KDE: Network Configuration: DNS .......... 634
Figure 445 Red Hat 9.0: KDE: Network Configuration: Activate .......... 634
Figure 446 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 .......... 635
Figure 447 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 .......... 635
Figure 448 Red Hat 9.0: DNS Settings in resolv.conf .......... 635
Figure 449 Red Hat 9.0: Restart Ethernet Card .......... 635
Figure 450 Red Hat 9.0: Checking TCP/IP Properties .......... 636
Figure 451 Pop-up Blocker .......... 637
Figure 452 Internet Options: Privacy .......... 638
Figure 453 Internet Options: Privacy .......... 639
Figure 454 Pop-up Blocker Settings .......... 639
Figure 455 Internet Options: Security .......... 640
Figure 456 Security Settings - Java Scripting .......... 641
Figure 457 Security Settings - Java .......... 641
Figure 458 Java (Sun) .......... 642
Figure 459 Mozilla Firefox: Tools > Options .......... 643
Figure 460 Mozilla Firefox Content Security .......... 643
Figure 461 Network Number and Host ID .......... 646
Figure 462 Subnetting Example: Before Subnetting .......... 648
Figure 463 Subnetting Example: After Subnetting .......... 649
Figure 464 Security Certificate .......... 657
Figure 465 Login Screen .......... 658
Figure 466 Certificate General Information before Import .......... 658
Figure 467 Certificate Import Wizard 1 .......... 659
Figure 468 Certificate Import Wizard 2 .......... 659

Figure 469 Certificate Import Wizard 3 .......... 660
Figure 470 Root Certificate Store .......... 660
Figure 471 Certificate General Information after Import .......... 661
Figure 472 ZyWALL Trusted CA Screen .......... 662
Figure 473 CA Certificate Example .......... 663
Figure 474 Personal Certificate Import Wizard 1 .......... 664
Figure 475 Personal Certificate Import Wizard 2 .......... 664
Figure 476 Personal Certificate Import Wizard 3 .......... 665
Figure 477 Personal Certificate Import Wizard 4 .......... 665
Figure 478 Personal Certificate Import Wizard 5 .......... 666
Figure 479 Personal Certificate Import Wizard 6 .......... 666
Figure 480 Access the ZyWALL Via HTTPS .......... 666
Figure 481 SSL Client Authentication .......... 667
Figure 482 ZyWALL Secure Login Screen .......... 667

# List of Tables

Table 1 Front Panel LEDs ........ 49
Table 2 Title Bar: Web Configurator Icons ........ 54
Table 3 Web Configurator HOME Screen in Router Mode ........ 55
Table 4 Web Configurator HOME Screen in Bridge Mode ........ 58
Table 5 Bridge and Router Mode Features Comparison ........ 60
Table 6 Screens Summary ........ 61
Table 7 HOME > Show Statistics ........ 64
Table 8 HOME > DHCP Table ........ 65
Table 9 HOME > VPN Status ........ 66
Table 10 ADVANCED > BW MGMT > Monitor ........ 67
Table 11 ISP Parameters: Ethernet Encapsulation ........ 70
Table 12 ISP Parameters: PPPoE Encapsulation ........ 72
Table 13 ISP Parameters: PPTP Encapsulation ........ 74
Table 14 Internet Access Wizard: Registration ........ 77
Table 15 VPN Wizard: Gateway Setting ........ 80
Table 16 VPN Wizard: Network Setting ........ 81
Table 17 VPN Wizard: IKE Tunnel Setting ........ 83
Table 18 VPN Wizard: IPSec Setting ........ 84
Table 19 VPN Wizard: VPN Status ........ 86
Table 20 REGISTRATION ........ 128
Table 21 REGISTRATION > Service ........ 130
Table 22 NETWORK > LAN ........ 137
Table 23 NETWORK > LAN > Static DHCP ........ 140
Table 24 NETWORK > LAN > IP Alias ........ 141
Table 25 NETWORK > LAN > Port Roles ........ 142
Table 26 STP Path Costs ........ 146
Table 27 STP Port States ........ 147
Table 28 NETWORK > Bridge ........ 148
Table 29 NETWORK > Bridge > Port Roles ........ 150
Table 30 NETWORK > WAN Route ........ 152
Table 31 Private IP Address Ranges ........ 153
Table 32 NETWORK > WAN > WAN (Ethernet Encapsulation) ........ 155
Table 33 NETWORK > WAN > WAN (PPPoE Encapsulation) ........ 158
Table 34 NETWORK > WAN > WAN (PPTP Encapsulation) ........ 161
Table 35 NETWORK > WAN > Traffic Redirect ........ 165
Table 36 NETWORK > WAN > Dial Backup ........ 166
Table 37 NETWORK > WAN > Dial Backup > Edit ........ 169
Table 38 NETWORK > DMZ ........ 172

Table 39 NETWORK > DMZ > Static DHCP ........ 175
Table 40 NETWORK > DMZ > IP Alias ........ 176
Table 41 NETWORK > DMZ > Port Roles ........ 179
Table 42 NETWORK > WLAN ........ 182
Table 43 NETWORK > WLAN > Static DHCP ........ 185
Table 44 NETWORK > WLAN > IP Alias ........ 186
Table 45 NETWORK > WLAN > Port Roles ........ 188
Table 46 Blocking All LAN to WAN IRC Traffic Example ........ 200
Table 47 Limited LAN to WAN IRC Traffic Example ........ 201
Table 48 SECURITY > FIREWALL > Default Rule (Router Mode) ........ 203
Table 49 SECURITY > FIREWALL > Default Rule (Bridge Mode) ........ 205
Table 50 SECURITY > FIREWALL > Rule Summary ........ 207
Table 51 SECURITY > FIREWALL > Rule Summary > Edit ........ 210
Table 52 SECURITY > FIREWALL > Anti-Probing ........ 212
Table 53 SECURITY > FIREWALL > Threshold ........ 214
Table 54 SECURITY > FIREWALL > Service ........ 215
Table 55 SECURITY > FIREWALL > Service > Add ........ 216
Table 56 SECURITY > CONTENT FILTER > General ........ 225
Table 57 SECURITY > CONTENT FILTER > Policy ........ 228
Table 58 SECURITY > CONTENT FILTER > Policy > General ........ 229
Table 59 SECURITY > CONTENT FILTER > Policy > External Database ........ 231
Table 60 SECURITY > CONTENT FILTER > Policy > Customization ........ 238
Table 61 SECURITY > CONTENT FILTER > Policy > Schedule ........ 240
Table 62 SECURITY > CONTENT FILTER > Object ........ 241
Table 63 SECURITY > CONTENT FILTER > Cache ........ 244
Table 64 SECURITY > VPN > VPN Rules (IKE) ........ 256
Table 65 VPN Example: Matching ID Type and Content ........ 259
Table 66 VPN Example: Mismatching ID Type and Content ........ 259
Table 67 SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy ........ 266
Table 68 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy ........ 275
Table 69 SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding ........ 279
Table 70 SECURITY > VPN > VPN Rules (IKE) > Move Network Policy ........ 280
Table 71 SECURITY > VPN > VPN Rules (Manual) ........ 282
Table 72 SECURITY > VPN > VPN Rules (Manual) > Edit ........ 283
Table 73 SECURITY > VPN > SA Monitor ........ 286
Table 74 SECURITY > VPN > Global Setting ........ 288
Table 75 Telecommuters Sharing One VPN Rule Example ........ 290
Table 76 Telecommuters Using Unique VPN Rules Example ........ 291
Table 77 SECURITY > CERTIFICATES > My Certificates ........ 298
Table 78 SECURITY > CERTIFICATES > My Certificates > Details ........ 300
Table 79 SECURITY > CERTIFICATES > My Certificates > Export ........ 303
Table 80 SECURITY > CERTIFICATES > My Certificates > Import ........ 304
Table 81 SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12 ........ 305

Table 82 SECURITY > CERTIFICATES > My Certificates > Create ................................................ 307
Table 83 SECURITY > CERTIFICATES > Trusted CAs ..........................................................................311
Table 84 SECURITY > CERTIFICATES > Trusted CAs > Details ..................................................... 313
Table 85 SECURITY > CERTIFICATES > Trusted CAs Import ........................................................ 315
Table 86 SECURITY > CERTIFICATES > Trusted Remote Hosts .................................................... 316
Table 87 SECURITY > CERTIFICATES > Trusted Remote Hosts > Details ..................................... 317
Table 88 SECURITY > CERTIFICATES > Trusted Remote Hosts > Import ...................................... 319
Table 89 SECURITY > CERTIFICATES > Directory Servers ........................................................... 320
Table 90 SECURITY > CERTIFICATES > Directory Server > Add .................................................. 321
Table 91 SECURITY > AUTH SERVER > Local User Database ...................................................... 325
Table 92 SECURITY > AUTH SERVER > RADIUS ........................................................................... 326
Table 93 NAT Definitions ..................................................................................................................... 331
Table 94 NAT Mapping Types ............................................................................................................. 335
Table 95 ADVANCED > NAT > NAT Overview .................................................................................. 336
Table 96 ADVANCED > NAT > Address Mapping ............................................................................. 338
Table 97 ADVANCED > NAT > Address Mapping > Edit .................................................................. 340
Table 98 ADVANCED > NAT > Port Forwarding ................................................................................ 343
Table 99 ADVANCED > NAT > Port Triggering .................................................................................. 345
Table 100 ADVANCED > STATIC ROUTE > IP Static Route ........................................................... 348
Table 101 ADVANCED > STATIC ROUTE > IP Static Route > Edit ................................................. 349
Table 102 Application and Subnet-based Bandwidth Management Example .................................... 352
Table 103 Maximize Bandwidth Usage Example ................................................................................ 354
Table 104 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example ........................ 354
Table 105 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example ..................... 355
Table 106 Bandwidth Borrowing Example ........................................................................................... 356
Table 107 Over Allotment of Bandwidth Example ............................................................................... 356
Table 108 ADVANCED > BW MGMT > Summary ............................................................................... 357
Table 109 ADVANCED > BW MGMT > Class Setup ........................................................................... 359
Table 110 ADVANCED > BW MGMT > Class Setup > Add Sub-Class ............................................... 360
Table 111 Services and Port Numbers ................................................................................................ 362
Table 112 ADVANCED > BW MGMT > Class Setup > Statistics ........................................................ 363
Table 113 ADVANCED > BW MGMT > Monitor ................................................................................... 364
Table 114 ADVANCED > DNS > System DNS .................................................................................... 368
Table 115 ADVANCED > DNS > Add (Address Record) ..................................................................... 369
Table 116 ADVANCED > DNS > Insert (Name Server Record) ........................................................... 370
Table 117 ADVANCED > DNS > Cache ............................................................................................... 372
Table 118 ADVANCED > DNS > DHCP ............................................................................................... 373
Table 119 ADVANCED > DNS > DDNS ............................................................................................... 375
Table 120 ADVANCED > REMOTE MGMT > WWW ........................................................................... 380
Table 121 ADVANCED > REMOTE MGMT > SSH .............................................................................. 387
Table 122 ADVANCED > REMOTE MGMT > TELNET ........................................................................ 390
Table 123 ADVANCED > REMOTE MGMT > FTP ............................................................................... 391
Table 124 SNMP Traps ........................................................................................................................ 393

Table 125 ADVANCED > REMOTE MGMT > SNMP .......... 394
Table 126 ADVANCED > REMOTE MGMT > DNS .......... 395
Table 127 ADVANCED > REMOTE MGMT > CNM .......... 396
Table 128 ADVANCED > UPnP .......... 400
Table 129 ADVANCED > UPnP > Ports .......... 401
Table 130 ADVANCED > Custom APP .......... 410
Table 131 ADVANCED > ALG .......... 415
Table 132 LOGS > View Log .......... 420
Table 133 Log Description Example .......... 420
Table 134 LOGS > Log Settings .......... 424
Table 135 LOGS > Reports .......... 426
Table 136 LOGS > Reports: Web Site Hits Report .......... 427
Table 137 LOGS > Reports: Host IP Address .......... 428
Table 138 LOGS > Reports: Protocol/ Port .......... 429
Table 139 Report Specifications .......... 430
Table 140 System Maintenance Logs .......... 430
Table 141 System Error Logs .......... 432
Table 142 Access Control Logs .......... 432
Table 143 TCP Reset Logs .......... 433
Table 144 Packet Filter Logs .......... 433
Table 145 ICMP Logs .......... 433
Table 146 CDR Logs .......... 434
Table 147 PPP Logs .......... 434
Table 148 UPnP Logs .......... 434
Table 149 Content Filtering Logs .......... 435
Table 150 Attack Logs .......... 435
Table 151 Remote Management Logs .......... 437
Table 152 IPSec Logs .......... 437
Table 153 IKE Logs .......... 438
Table 154 PKI Logs .......... 441
Table 155 Certificate Path Verification Failure Reason Codes .......... 442
Table 156 ACL Setting Notes .......... 442
Table 157 ICMP Notes .......... 443
Table 158 Syslog Logs .......... 445
Table 159 RFC-2408 ISAKMP Payload Types .......... 446
Table 160 MAINTENANCE > General Setup .......... 448
Table 161 MAINTENANCE > Password .......... 449
Table 162 MAINTENANCE > Time and Date .......... 450
Table 163 MAC-address-to-port Mapping Table .......... 453
Table 164 MAINTENANCE > Device Mode (Router Mode) .......... 455
Table 165 MAINTENANCE > Device Mode (Bridge Mode) .......... 456
Table 166 MAINTENANCE > Firmware Upload .......... 458
Table 167 Restore Configuration .......... 460

Table 168 MAINTENANCE > Diagnostics .......... 463
Table 169 Main Menu Commands .......... 468
Table 170 Main Menu Summary .......... 470
Table 171 SMT Menus Overview .......... 471
Table 172 Menu 1: General Setup (Router Mode) .......... 475
Table 173 Menu 1: General Setup (Bridge Mode) .......... 476
Table 174 Menu 1.1: Configure Dynamic DNS .......... 477
Table 175 Menu 1.1.1: DDNS Host Summary .......... 478
Table 176 Menu 1.1.1: DDNS Edit Host .......... 479
Table 177 MAC Address Cloning in WAN Setup .......... 482
Table 178 Menu 2: Dial Backup Setup .......... 483
Table 179 Advanced WAN Port Setup: AT Commands Fields .......... 484
Table 180 Advanced WAN Port Setup: Call Control Parameters .......... 485
Table 181 Menu 11.3: Remote Node Profile (Backup ISP) .......... 486
Table 182 Menu 11.2.2: Remote Node Network Layer Options .......... 487
Table 183 Menu 11.2.3: Remote Node Script .......... 489
Table 184 Menu 3.2: DHCP Ethernet Setup Fields .......... 493
Table 185 Menu 3.2: LAN TCP/IP Setup Fields .......... 494
Table 186 Menu 3.2.1: IP Alias Setup .......... 495
Table 187 Menu 4: Internet Access Setup (Ethernet) .......... 498
Table 188 New Fields in Menu 4 (PPTP) Screen .......... 499
Table 189 New Fields in Menu 4 (PPPoE) screen .......... 500
Table 190 Menu 11.1: Remote Node Profile for Ethernet Encapsulation .......... 510
Table 191 Fields in Menu 11.1 (PPPoE Encapsulation Specific) .......... 513
Table 192 Menu 11.1: Remote Node Profile for PPTP Encapsulation .......... 514
Table 193 Remote Node Network Layer Options Menu Fields .......... 515
Table 194 Menu 11.1.5: Traffic Redirect Setup .......... 517
Table 195 Menu 12. 1: Edit IP Static Route .......... 520
Table 196 Applying NAT in Menus 4 & 11.1.2 .......... 523
Table 197 SUA Address Mapping Rules .......... 525
Table 198 Fields in Menu 15.1.1 .......... 526
Table 199 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set .......... 527
Table 200 15.2.1: NAT Server Configuration .......... 529
Table 201 Menu 15.3: Trigger Port Setup .......... 538
Table 202 Abbreviations Used in the Filter Rules Summary Menu .......... 545
Table 203 Rule Abbreviations Used .......... 545
Table 204 Menu 21.1.1.1: TCP/IP Filter Rule .......... 547
Table 205 Generic Filter Rule Menu Fields .......... 549
Table 206 SNMP Configuration Menu Fields .......... 557
Table 207 SNMP Traps .......... 558
Table 208 System Maintenance: Status Menu Fields .......... 560
Table 209 Fields in System Maintenance: Information .......... 562
Table 210 System Maintenance Menu Syslog Parameters .......... 564

Table 211 System Maintenance Menu Diagnostic ........ 568
Table 212 Filename Conventions ........ 572
Table 213 General Commands for GUI-based FTP Clients ........ 574
Table 214 General Commands for GUI-based TFTP Clients ........ 575
Table 215 Valid Commands ........ 588
Table 216 Budget Management ........ 590
Table 217 Call History ........ 591
Table 218 Menu 24.10 System Maintenance: Time and Date Setting ........ 592
Table 219 Menu 24.11 – Remote Management Control ........ 596
Table 220 Schedule Set Setup ........ 600
Table 221 Hardware Specifications ........ 613
Table 222 Firmware Specifications ........ 613
Table 223 Feature and Performance Specifications ........ 615
Table 224 Console Cable Pin Assignments ........ 616
Table 225 Dial Backup Cable Pin Assignments ........ 616
Table 226 Ethernet Cable Pin Assignments ........ 616
Table 227 IP Address Network Number and Host ID Example ........ 646
Table 228 Subnet Masks ........ 647
Table 229 Maximum Host Numbers ........ 647
Table 230 Alternative Subnet Mask Notation ........ 647
Table 231 Subnet 1 ........ 649
Table 232 Subnet 2 ........ 650
Table 233 Subnet 3 ........ 650
Table 234 Subnet 4 ........ 650
Table 235 Eight Subnets ........ 650
Table 236 24-bit Network Number Subnet Planning ........ 651
Table 237 16-bit Network Number Subnet Planning ........ 651
Table 238 Commonly Used Services ........ 654

# PART I

# Introduction and Registration

Getting to Know Your ZyWALL (47)

Introducing the Web Configurator (51)

Wizard Setup (69)

Tutorials (89)

Registration (127)

# 1

# Getting to Know Your ZyWALL

This chapter introduces the main features and applications of the ZyWALL.

## 1.1 ZyWALL Internet Security Appliance Overview

The ZyWALL is loaded with security features including VPN, firewall, content filtering and certificates. The ZyWALL's De-Militarized Zone (DMZ) increases LAN security by providing separate ports for connecting publicly accessible servers. The ZyWALL provides the option to change port roles from LAN to DMZ.

You can also deploy the ZyWALL as a transparent firewall in an existing network with minimal configuration.

The ZyWALL provides bandwidth management, NAT, port forwarding, DHCP server and many other powerful features.

You can add an IEEE 802.11a/b/g-compliant wireless LAN by connecting an access point (AP) to an Ethernet port in a WLAN port role.

See Chapter 46 on page 613 for a complete list of features.

## 1.2 Applications for the ZyWALL

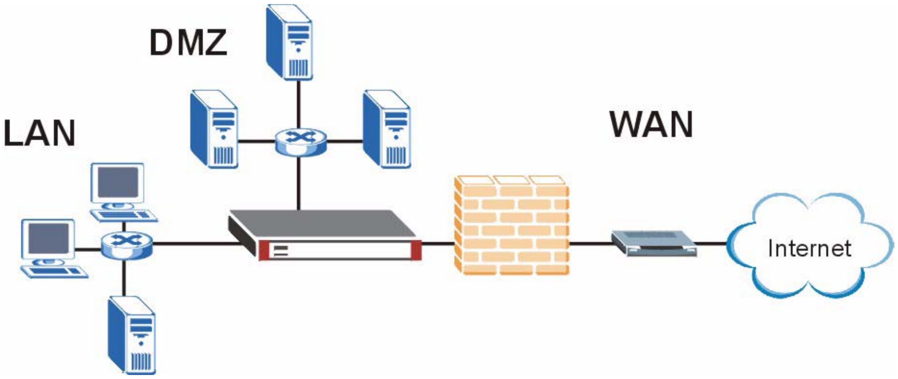
Here are some examples of what you can do with your ZyWALL.

### 1.2.1 Secure Broadband Internet Access via Cable or DSL Modem

For Internet access, connect the WAN Ethernet port to your existing Internet access gateway (company network, or your cable or DSL modem for example). Connect computers or servers to the LAN ports for shared Internet access.

The ZyWALL guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

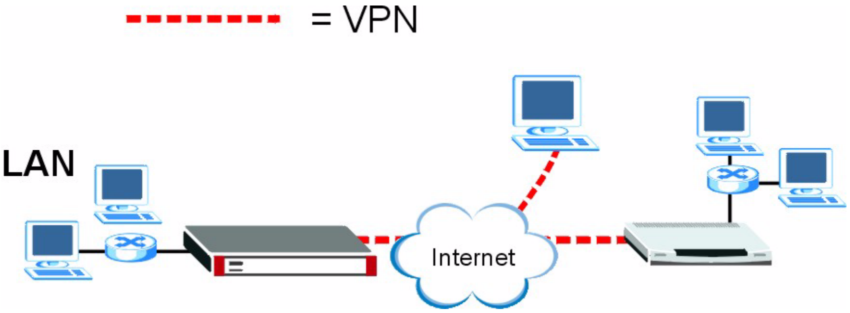
**Figure 1** Secure Internet Access via Cable, DSL or Wireless Modem



## 1.2.2 VPN Application

ZyWALL VPN is an ideal cost-effective way to connect branch offices, business partners and telecommuters over the Internet without the need (and expense) for leased lines between sites.

**Figure 2** VPN Application



# 1.3 Ways to Manage the ZyWALL

Use any of the following methods to manage the ZyWALL.

- Web Configurator. This is recommended for everyday management of the ZyWALL using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device.
- FTP for firmware upgrades and configuration backup/restore (Chapter 41 on page 571)
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.
- Vantage CNM (Centralized Network Management). The device can be remotely managed using a Vantage CNM server.

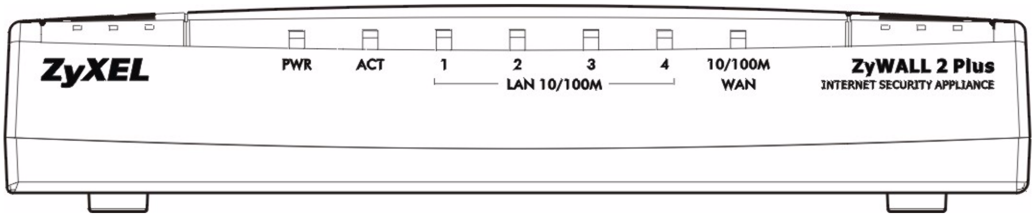
## 1.4 Good Habits for Managing the ZyWALL

Do the following things regularly to make the ZyWALL more secure and to manage the ZyWALL more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyWALL to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyWALL. You could simply restore your last configuration.

## 1.5 LEDs

**Figure 3** Front Panel



The following table describes the lights.

**Table 1** Front Panel LEDs

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| **PWR** | | Off | The ZyWALL is turned off. |
| | Green | On | The ZyWALL is ready and running. |
| | | Flashing | The ZyWALL is restarting. |
| | Red | On | The power to the ZyWALL is too low. |
| **ACT** | Green | Off | The backup port is not connected. |
| | | On | The backup port is connected. |
| | | Flashing | The backup port is sending or receiving packets. |
| **LAN 10/100** | | Off | The LAN/DMZ/WLAN is not connected. |
| | Green | On | The ZyWALL has a successful 10Mbps Ethernet connection. |
| | | Flashing | The 10M LAN/DMZ/WLAN is sending or receiving packets. |
| | Orange | On | The ZyWALL has a successful 100Mbps Ethernet connection. |
| | | Flashing | The 100M LAN/DMZ/WLAN is sending or receiving packets. |

**Table 1** Front Panel LEDs (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| **WAN 10/100** | | Off | The WAN connection is not ready, or has failed. |
| | Green | On | The ZyWALL has a successful 10Mbps WAN connection. |
| | | Flashing | The 10M WAN is sending or receiving packets. |
| | Orange | On | The ZyWALL has a successful 100Mbps WAN connection. |
| | | Flashing | The 100M WAN is sending or receiving packets. |

# 2

# Introducing the Web Configurator

This chapter describes how to access the ZyWALL web configurator and provides an overview of its screens.

## 2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyWALL setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See Appendix B on page 637 if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

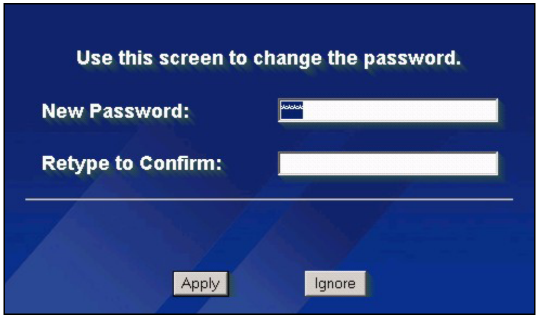
## 2.2 Accessing the ZyWALL Web Configurator

By default, the packets from WLAN to WLAN/ZyWALL are dropped and users cannot configure the ZyWALL wirelessly.

1. Make sure your ZyWALL hardware is properly connected and prepare your computer/ computer network to connect to the ZyWALL (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

**Figure 4** Change Password Screen



Use this screen to change the password.

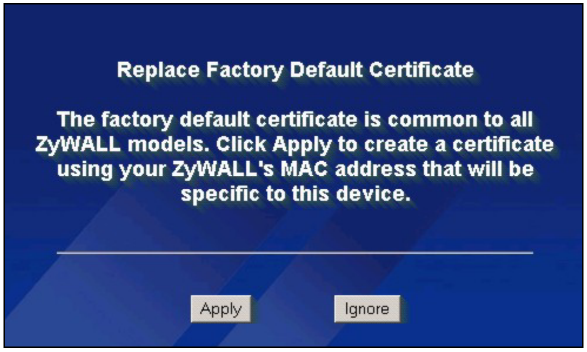
New Password:

Retype to Confirm:

6 Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyWALL's MAC address that will be specific to this device.

If you do not replace the default certificate here or in the **CERTIFICATES** screen, this screen displays every time you access the web configurator.

**Figure 5** Replace Certificate Screen



Replace Factory Default Certificate

The factory default certificate is common to all ZyWALL models. Click Apply to create a certificate using your ZyWALL's MAC address that will be specific to this device.

7 You should now see the **HOME** screen (see Figure 8 on page 55).

The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the ZyWALL if this happens to you.

## 2.3 Resetting the ZyWALL

If you forget your password or cannot access the web configurator, you will need to reload the factory-default configuration file or use the **RESET** button on the back of the ZyWALL. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to 1234, also.

### 2.3.1 Procedure To Use The Reset Button

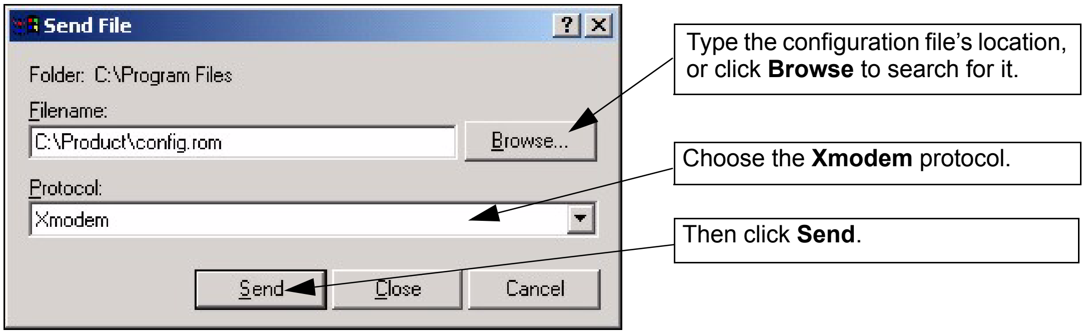
Make sure the **PWR** LED is on (not blinking) before you begin this procedure.

1. Press the **RESET** button for ten seconds, and then release it. If the **PWR** LED begins to blink, the defaults have been restored and the ZyWALL restarts. Otherwise, go to step 2.
2. Turn the ZyWALL off.
3. While pressing the **RESET** button, turn the ZyWALL on.
4. Continue to hold the **RESET** button. The **PWR** LED will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the ZyWALL is now restarting.
5. Release the **RESET** button and wait for the ZyWALL to finish restarting.

### 2.3.2 Uploading a Configuration File Via Console Port

1. Download the default configuration file from the ZyXEL FTP site, unzip it and save it in a folder.
2. Turn off the ZyWALL, begin a terminal emulation software session and turn on the ZyWALL again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.
3. Enter "y" at the prompt below to go into debug mode.
4. Enter "atlc" after "Enter Debug Mode" message.
5. Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

**Figure 6** Example Xmodem Upload



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

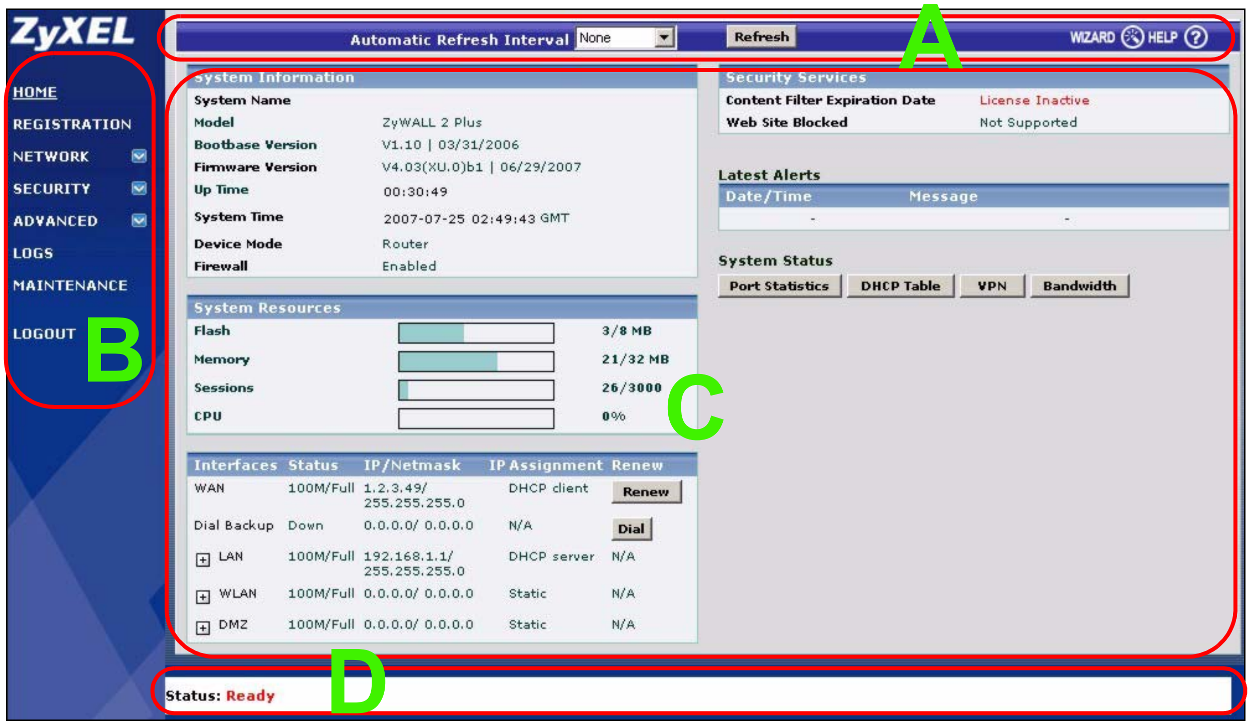
Then click **Send**.

6. After successful firmware upload, enter "atgo" to restart the router.

## 2.4 Navigating the ZyWALL Web Configurator

The following summarizes how to navigate the web configurator from the **HOME** screen. This guide uses the ZyWALL 70 screenshots as an example. The screens may vary slightly for different ZyWALL models.

**Figure 7** HOME Screen


ZyXEL
Automatic Refresh Interval
None
Refresh
WIZARD
HELP
HOME
REGISTRATION
NETWORK
SECURITY
ADVANCED
LOGS
MAINTENANCE
LOGOUT
System Status
Port Statistics
DHCP Table
VPN
Bandwidth
Renew
Dial
A
B
C
D

| System Information | |
|---|---|
| System Name | |
| Model | ZyWALL 2 Plus |
| Bootbase Version | V1.10 \| 03/31/2006 |
| Firmware Version | V4.03(XU.0)b1 \| 06/29/2007 |
| Up Time | 00:30:49 |
| System Time | 2007-07-25 02:49:43 GMT |
| Device Mode | Router |
| Firewall | Enabled |

| Security Services | |
|---|---|
| Content Filter Expiration Date | License Inactive |
| Web Site Blocked | Not Supported |

Latest Alerts

| Date/Time | Message |
|---|---|
| - | - |

| System Resources | |
|---|---|
| Flash | 3/8 MB |
| Memory | 21/32 MB |
| Sessions | 26/3000 |
| CPU | 0% |

| Interfaces | Status | IP/Netmask | IP Assignment | Renew |
|---|---|---|---|---|
| WAN | 100M/Full | 1.2.3.49/ 255.255.255.0 | DHCP client | Renew |
| Dial Backup | Down | 0.0.0.0/ 0.0.0.0 | N/A | Dial |
| ⊞ LAN | 100M/Full | 192.168.1.1/ 255.255.255.0 | DHCP server | N/A |
| ⊞ WLAN | 100M/Full | 0.0.0.0/ 0.0.0.0 | Static | N/A |
| ⊞ DMZ | 100M/Full | 0.0.0.0/ 0.0.0.0 | Static | N/A |

Status: Ready

As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

### 2.4.1 Title Bar

The title bar provides some icons in the upper right corner.

The icons provide the following functions.

**Table 2** Title Bar: Web Configurator Icons

| ICON | DESCRIPTION |
|---|---|
| WIZARD | **Wizard**: Click this icon to open one of the web configurator wizards. See Chapter 3 on page 69 for more information. |
| HELP ? | **Help**: Click this icon to open the help page for the current screen. |

## 2.4.2 Main Window

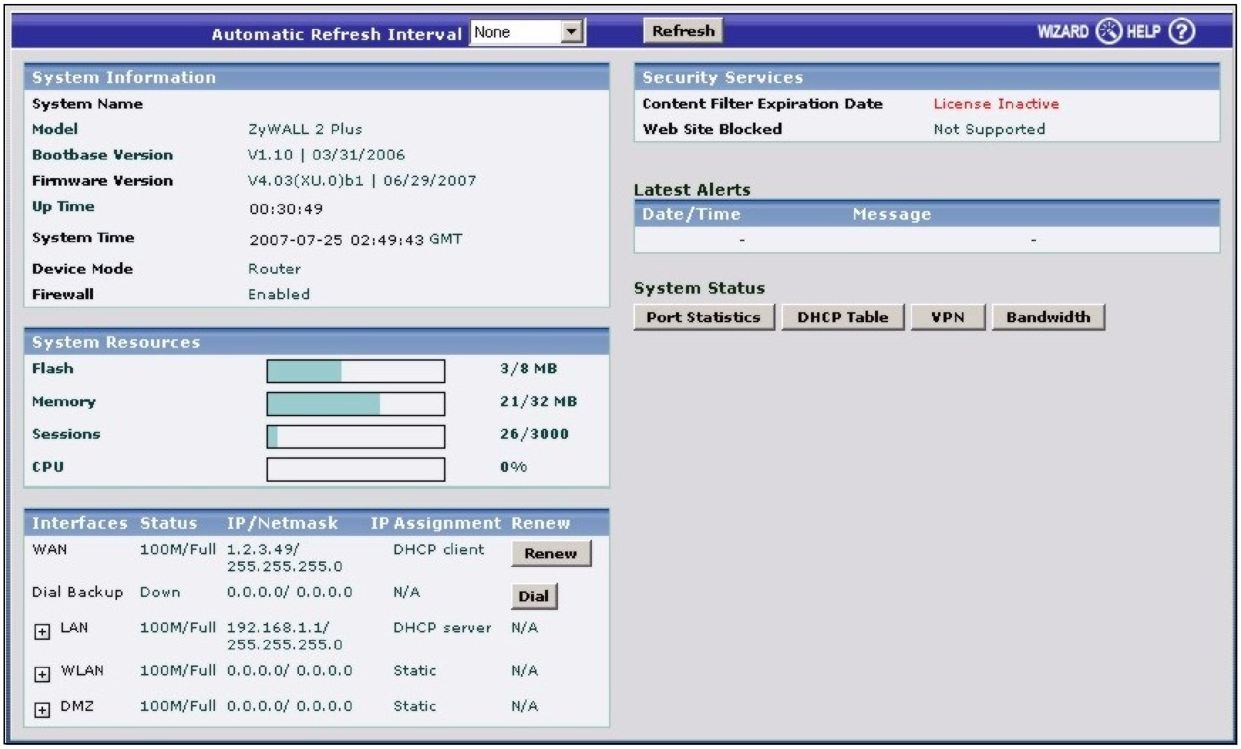
The main window shows the screen you select in the navigation panel. It is discussed in more detail in the rest of this document.

Right after you log in, the **HOME** screen is displayed. The screen varies according to the device mode you select in the **MAINTENANCE > Device Mode** screen.

## 2.4.3 HOME Screen: Router Mode

The following screen displays when the ZyWALL is set to router mode. This screen displays general status information about the ZyWALL. The ZyWALL is set to router mode by default.

**Figure 8** Web Configurator HOME Screen in Router Mode



Automatic Refresh Interval: None

**System Information**

| | |
|---|---|
| System Name | |
| Model | ZyWALL 2 Plus |
| Bootbase Version | V1.10 \| 03/31/2006 |
| Firmware Version | V4.03(XU.0)b1 \| 06/29/2007 |
| Up Time | 00:30:49 |
| System Time | 2007-07-25 02:49:43 GMT |
| Device Mode | Router |
| Firewall | Enabled |

**Security Services**

| | |
|---|---|
| Content Filter Expiration Date | License Inactive |
| Web Site Blocked | Not Supported |

**Latest Alerts**

| Date/Time | Message |
|---|---|
| - | - |

**System Resources**

| | |
|---|---|
| Flash | 3/8 MB |
| Memory | 21/32 MB |
| Sessions | 26/3000 |
| CPU | 0% |

| Interfaces | Status | IP/Netmask | IP Assignment | Renew |
|---|---|---|---|---|
| WAN | 100M/Full | 1.2.3.49/<br>255.255.255.0 | DHCP client | Renew |
| Dial Backup | Down | 0.0.0.0/ 0.0.0.0 | N/A | Dial |
| ⊞ LAN | 100M/Full | 192.168.1.1/<br>255.255.255.0 | DHCP server | N/A |
| ⊞ WLAN | 100M/Full | 0.0.0.0/ 0.0.0.0 | Static | N/A |
| ⊞ DMZ | 100M/Full | 0.0.0.0/ 0.0.0.0 | Static | N/A |

The following table describes the labels in this screen.

**Table 3** Web Configurator HOME Screen in Router Mode

| LABEL | DESCRIPTION |
|---|---|
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the status screen statistics immediately. |
| System Information | |
| System Name | This is the **System Name** you enter in the **MAINTENANCE > General** screen. It is for identification purposes. Click the field label to go to the screen where you can specify a name for this ZyWALL. |
| Model | This is the model name of your ZyWALL. |
| Bootbase Version | This is the bootbase version and the date created. |

**Table 3** Web Configurator HOME Screen in Router Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Firmware Version | This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. Click the field label to go to the screen where you can upload a new firmware file. |
| Up Time | This field displays how long the ZyWALL has been running since it last started up. The ZyWALL starts up when you turn it on, when you restart it (**MAINTENANCE > Restart**), or when you reset it (see Section 2.3 on page 53). |
| System Time | This field displays your ZyWALL's present date (in yyyy-mm-dd format) and time (in hh:mm:ss format) along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the ZyWALL to use it. Click the field label to go to the screen where you can modify the ZyWALL's date and time settings. |
| Device Mode | This displays whether the ZyWALL is functioning as a router or a bridge. Click the field label to go to the screen where you can configure the ZyWALL as a router or a bridge. |
| Firewall | This displays whether or not the ZyWALL's firewall is activated. Click the field label to go to the screen where you can turn the firewall on or off. |
| System Resources | |
| Flash | The first number shows how many megabytes of the flash the ZyWALL is using. |
| Memory | The first number shows how many megabytes of the heap memory the ZyWALL is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall.<br>The second number shows the ZyWALL's total heap memory (in megabytes).<br>The bar displays what percent of the ZyWALL's heap memory is in use. The bar turns from green to red when the maximum is being approached. |
| Sessions | The first number shows how many sessions are currently open on the ZyWALL. This includes all sessions that are currently traversing the ZyWALL, terminating at the ZyWALL or Initiated from the ZyWALL.<br>The second number is the maximum number of sessions that can be open at one time.<br>The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached. |
| CPU | This field displays what percentage of the ZyWALL's processing ability is currently used. When this percentage is close to 100%, the ZyWALL is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management. |
| Interfaces | This is the port type.<br>Click "+" to expand or "-" to collapse the IP alias drop-down lists. |
| Status | For the LAN, DMZ and WLAN ports, this displays the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.<br>For the WAN and Dial Backup ports, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation. |
| IP/Netmask | This shows the port's IP address and subnet mask. |

**Table 3** Web Configurator HOME Screen in Router Mode (continued)

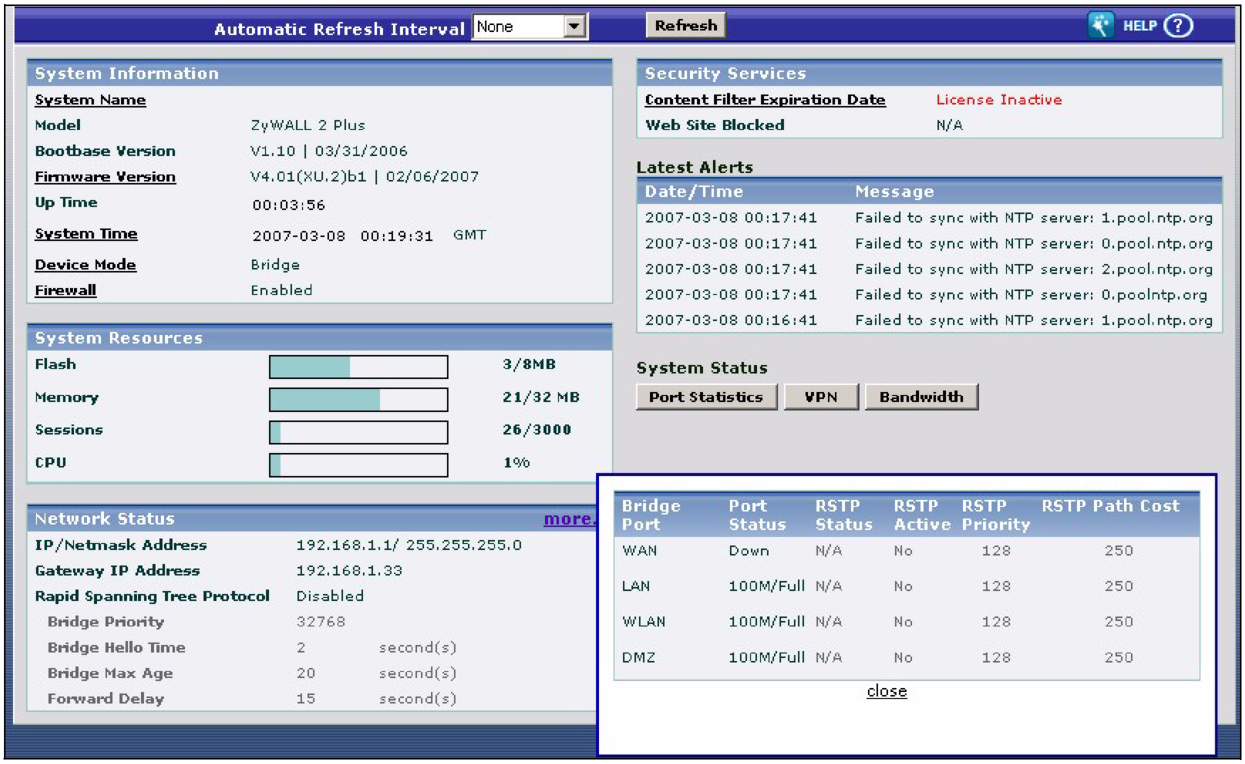
| LABEL | DESCRIPTION |
|---|---|
| IP Assignment | For the WAN, if the ZyWALL gets its IP address automatically from an ISP, this displays **DHCP client** when you're using Ethernet encapsulation and **IPCP Client** when you're using PPPoE or PPTP encapsulation. **Static** displays if the WAN port is using a manually entered static (fixed) IP address.<br>For the LAN, **DHCP server** displays when the ZyWALL is set to automatically give IP address information to the computers connected to the LAN. **DHCP relay** displays when the ZyWALL is set to forward IP address assignment requests to another DHCP server. **Static** displays if the LAN port is using a manually entered static (fixed) IP address. In this case, you must have another DHCP server on your LAN, or else the computers must be manually configured.<br>For the dial backup port, this shows **N/A** when dial backup is disabled and **IPCP client** when dial backup is enabled. |
| Renew | If you are using Ethernet encapsulation and the WAN port is configured to get the IP address automatically from the ISP, click **Renew** to release the WAN port's dynamically assigned IP address and get the IP address afresh. Click **Dial** to dial up the PPTP, PPPoE or dial backup connection. Click **Drop** to disconnect the PPTP, PPPoE or dial backup connection. |
| Security Services | |
| Content Filter Expiration Date | This is the date the category-based content filtering service subscription expires. Click the field label to go to the screen where you can update your service subscription. |
| Web Site Blocked | This displays how many web site hits the ZyWALL has blocked since it last started up. N/A displays when the service subscription has expired. |
| Latest Alerts | This table displays the five most recent alerts recorded by the ZyWALL. You can see more information in the **View Log** screen, such as the source and destination IP addresses and port numbers of the incoming packets. |
| Date/Time | This is the date and time the alert was recorded. |
| Message | This is the reason for the alert. |
| System Status | |
| Port Statistics | Click **Port Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port. |
| DHCP Table | Click **DHCP Table** to show current DHCP client information. |
| VPN | Click **VPN** to display the active VPN connections. |
| Bandwidth | Click **Bandwidth** to view the ZyWALL's bandwidth usage and allotments. |

## 2.4.4 HOME Screen: Bridge Mode

The following screen displays when the ZyWALL is set to bridge mode. In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.

In bridge mode, the ZyWALL cannot get an IP address from a DHCP server. The LAN, WAN, DMZ and WLAN interfaces all have the same (static) IP address and subnet mask. You can configure the ZyWALL's IP address in order to access the ZyWALL for management. If you connect your computer directly to the ZyWALL, you also need to assign your computer a static IP address in the same subnet as the ZyWALL's IP address in order to access the ZyWALL.

You can use the firewall and VPN in bridge mode. See the user's guide for a list of other features that are available in bridge mode.



System Information

| | |
|---|---|
| System Name | |
| Model | ZyWALL 2 Plus |
| Bootbase Version | V1.10 \| 03/31/2006 |
| Firmware Version | V4.01(XU.2)b1 \| 02/06/2007 |
| Up Time | 00:03:56 |
| System Time | 2007-03-08 00:19:31 GMT |
| Device Mode | Bridge |
| Firewall | Enabled |

Security Services

| | |
|---|---|
| Content Filter Expiration Date | License Inactive |
| Web Site Blocked | N/A |

Latest Alerts

| Date/Time | Message |
|---|---|
| 2007-03-08 00:17:41 | Failed to sync with NTP server: 1.pool.ntp.org |
| 2007-03-08 00:17:41 | Failed to sync with NTP server: 0.pool.ntp.org |
| 2007-03-08 00:17:41 | Failed to sync with NTP server: 2.pool.ntp.org |
| 2007-03-08 00:17:41 | Failed to sync with NTP server: 0.poolntp.org |
| 2007-03-08 00:16:41 | Failed to sync with NTP server: 1.pool.ntp.org |

System Resources

| | |
|---|---|
| Flash | 3/8MB |
| Memory | 21/32 MB |
| Sessions | 26/3000 |
| CPU | 1% |

Network Status

| | | |
|---|---|---|
| IP/Netmask Address | 192.168.1.1/ 255.255.255.0 | |
| Gateway IP Address | 192.168.1.33 | |
| Rapid Spanning Tree Protocol | Disabled | |
| Bridge Priority | 32768 | |
| Bridge Hello Time | 2 | second(s) |
| Bridge Max Age | 20 | second(s) |
| Forward Delay | 15 | second(s) |

| Bridge Port | Port Status | RSTP Status | RSTP Active | RSTP Priority | RSTP Path Cost |
|---|---|---|---|---|---|
| WAN | Down | N/A | No | 128 | 250 |
| LAN | 100M/Full | N/A | No | 128 | 250 |
| WLAN | 100M/Full | N/A | No | 128 | 250 |
| DMZ | 100M/Full | N/A | No | 128 | 250 |

**Figure 9** Web Configurator HOME Screen in Bridge Mode

The following table describes the labels in this screen.

**Table 4** Web Configurator HOME Screen in Bridge Mode

| LABEL | DESCRIPTION |
|---|---|
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |
| System Information | |
| System Name | This is the **System Name** you enter in the **MAINTENANCE > General** screen. It is for identification purposes. Click the field label to go to the screen where you can specify a name for this ZyWALL. |
| Model | This is the model name of your ZyWALL. |
| Bootbase Version | This is the bootbase version and the date created. |
| Firmware Version | This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. Click the field label to go to the screen where you can upload a new firmware file. |
| Up Time | This field displays how long the ZyWALL has been running since it last started up. The ZyWALL starts up when you turn it on, when you restart it (**MAINTENANCE > Restart**), or when you reset it (see Section 2.3 on page 53). |

**Table 4** Web Configurator HOME Screen in Bridge Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| System Time | This field displays your ZyWALL’s present date (in yyyy-mm-dd format) and time (in hh:mm:ss format) along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the ZyWALL to use it. Click the field label to go to the screen where you can modify the ZyWALL’s date and time settings. |
| Device Mode | This displays whether the ZyWALL is functioning as a router or a bridge. Click the field label to go to the screen where you can configure the ZyWALL as a router or a bridge. |
| Firewall | This displays whether or not the ZyWALL’s firewall is activated. Click the field label to go to the screen where you can turn the firewall on or off. |
| System Resources | |
| Flash | The first number shows how many megabytes of the flash the ZyWALL is using. |
| Memory | The first number shows how many megabytes of the heap memory the ZyWALL is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall.<br>The second number shows the ZyWALL's total heap memory (in megabytes).<br>The bar displays what percent of the ZyWALL's heap memory is in use. The bar turns from green to red when the maximum is being approached. |
| Sessions | The first number shows how many sessions are currently open on the ZyWALL. This includes all sessions that are currently traversing the ZyWALL, terminating at the ZyWALL or initiated from the ZyWALL<br>The second number is the maximum number of sessions that can be open at one time.<br>The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached. |
| CPU | This field displays what percentage of the ZyWALL’s processing ability is currently used. When this percentage is close to 100%, the ZyWALL is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management. |
| Network Status | |
| IP/Netmask Address | This is the IP address and subnet mask of your ZyWALL in dotted decimal notation. |
| Gateway IP Address | This is the gateway IP address. |
| Rapid Spanning Tree Protocol | This shows whether RSTP (Rapid Spanning Tree Protocol) is active or not. The following labels or values relative to RSTP do not apply when RSTP is disabled. |
| Bridge Priority | This is the bridge priority of the ZyWALL. The bridge (or switch) with the lowest bridge priority value in the network is the root bridge (the base of the spanning tree). |
| Bridge Hello Time | This is the interval of BPDUs (Bridge Protocol Data Units) from the root bridge. |
| Bridge Max Age | This is the predefined interval that a bridge waits to get a Hello message (BPDU) from the root bridge. |
| Forward Delay | This is the forward delay interval. |
| Bridge Port | This is the port type. Port types are: **WAN**, **LAN**, **DMZ** and **WLAN**. |

**Table 4** Web Configurator HOME Screen in Bridge Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port Status | For the WAN, LAN, DMZ, and WLAN Interfaces, this displays the port speed and duplex setting. For the WAN port, it displays **Down** when the link is not ready or has failed. |
| RSTP Status | This is the RSTP status of the corresponding port. |
| RSTP Active | This shows whether or not RSTP is active on the corresponding port. |
| RSTP Priority | This is the RSTP priority of the corresponding port. |
| RSTP Path Cost | This is the cost of transmitting a frame from the root bridge to the corresponding port. |
| Security Services | |
| Content Filter Expiration Date | This is the date the category-based content filtering service subscription expires. Click the field label to go to the screen where you can update your service subscription. |
| Web Site Blocked | This displays how many web site hits the ZyWALL has blocked since it last started up. N/A displays when the service subscription has expired. |
| Latest Alerts | This table displays the five most recent alerts recorded by the ZyWALL. You can see more information in the **View Log** screen, such as the source and destination IP addresses and port numbers of the incoming packets. |
| Date/Time | This is the date and time the alert was recorded. |
| Message | This is the reason for the alert. |
| System Status | |
| Port Statistics | Click **Port Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port. |
| VPN | Click **VPN** to display the active VPN connections. |
| Bandwidth | Click **Bandwidth** to view the ZyWALL's bandwidth usage and allotments. |

## 2.4.5 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure ZyWALL features.

The following table lists the features available for each device mode. Not all ZyWALLs have all features listed in this table.

**Table 5** Bridge and Router Mode Features Comparison

| FEATURE | BRIDGE MODE | ROUTER MODE |
|---|---|---|
| Internet Access Wizard | | Y |
| VPN Wizard | Y | Y |
| DHCP Table | | Y |
| System Statistics | Y | Y |
| Registration | Y | Y |
| LAN | | Y |
| WAN | | Y |
| DMZ | | Y |
| Bridge | Y | |

**Table 5** Bridge and Router Mode Features Comparison

| FEATURE | BRIDGE MODE | ROUTER MODE |
|---|---|---|
| WLAN | | Y |
| Firewall | Y | Y |
| Content Filter | Y | Y |
| VPN | Y | Y |
| Certificates | Y | Y |
| Authentication Server | Y | Y |
| NAT | | Y |
| Static Route | | Y |
| Bandwidth Management | Y | Y |
| DNS | | Y |
| Remote Management | Y | Y |
| UPnP | | Y |
| Custom APP | Y | Y |
| ALG | Y | Y |
| Logs | Y | Y |
| Maintenance | Y | Y |

Table Key: A Y in a mode's column shows that the device mode has the specified feature. The information in this table was correct at the time of writing, although it may be subject to change.

The following table describes the sub-menus.

**Table 6** Screens Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| HOME | | This screen shows the ZyWALL's general device and network status information. Use this screen to access the wizards, statistics and DHCP table. |
| REGISTRATION | Registration | Use this screen to register your ZyWALL and activate the trial service subscriptions. |
| | Service | Use this to manage and update the service status and license information. |
| NETWORK | | |
| LAN | LAN | Use this screen to configure LAN DHCP and TCP/IP settings. |
| | Static DHCP | Use this screen to assign fixed IP addresses on the LAN. |
| | IP Alias | Use this screen to partition your LAN interface into subnets. |
| | Port Roles | Use this screen to change the LAN/DMZ/WLAN port roles. |
| BRIDGE | Bridge | Use this screen to change the bridge settings on the ZyWALL. |
| | Port Roles | Use this screen to change the LAN/DMZ/WLAN port roles on the ZyWALL. |

**Table 6** Screens Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| WAN | Route | This screen allows you to configure route priority. |
| | WAN | Use this screen to configure the WAN port for internet access. |
| | Traffic Redirect | Use this screen to configure your traffic redirect properties and parameters. |
| | Dial Backup | Use this screen to configure the backup WAN dial-up connection. |
| DMZ | DMZ | Use this screen to configure your DMZ connection. |
| | Static DHCP | Use this screen to assign fixed IP addresses on the DMZ. |
| | IP Alias | Use this screen to partition your DMZ interface into subnets. |
| | Port Roles | Use this screen to change the LAN/DMZ/WLAN port roles on the ZyWALL. |
| WLAN | WLAN | Use this screen to configure your WLAN connection. |
| | Static DHCP | Use this screen to assign fixed IP addresses on the WLAN. |
| | IP Alias | Use this screen to partition your WLAN interface into subnets. |
| | Port Roles | Use this screen to change the LAN/DMZ/WLAN port roles on the ZyWALL. |
| SECURITY | | |
| FIREWALL | Default Rule | Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule |
| | Rule Summary | This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule. |
| | Anti-Probing | Use this screen to change your anti-probing settings. |
| | Threshold | Use this screen to configure the threshold for DoS attacks. |
| | Service | Use this screen to configure custom services. |
| CONTENT FILTER | General | This screen allows you to enable content filtering and block certain web features. |
| | Policy | Use this screen to select which categories of web pages to filter out, as well as to register for external database content filtering and view reports. |
| | Object | Use this screen to customize the content filter list. |
| | Cache | Use this screen to view and configure the ZyWALL's URL caching. |
| VPN | VPN Rules (IKE) | Use this screen to configure VPN connections using IKE key management and view the rule summary. |
| | VPN Rules (Manual) | Use this screen to configure VPN connections using manual key management and view the rule summary. |
| | SA Monitor | Use this screen to display and manage active VPN connections. |
| | Global Setting | Use this screen to configure the IPSec timer settings. |
| CERTIFICATES | My Certificates | Use this screen to view a summary list of certificates and manage certificates and certification requests. |
| | Trusted CAs | Use this screen to view and manage the list of the trusted CAs. |
| | Trusted Remote Hosts | Use this screen to view and manage the certificates belonging to the trusted remote hosts. |
| | Directory Servers | Use this screen to view and manage the list of the directory servers. |

**Table 6** Screens Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| AUTH SERVER | Local User Database | Use this screen to configure the local user account(s) on the ZyWALL. |
| | RADIUS | Configure this screen to use an external server to authenticate wireless and/or VPN users. |
| ADVANCED | | |
| NAT | NAT Overview | Use this screen to enable NAT. |
| | Address Mapping | Use this screen to configure network address translation mapping rules. |
| | Port Forwarding | Use this screen to configure servers behind the ZyWALL. |
| | Port Triggering | Use this screen to change your ZyWALL's port triggering settings. |
| STATIC ROUTE | IP Static Route | Use this screen to configure IP static routes. |
| BW MGMT | Summary | Use this screen to enable bandwidth management on an interface. |
| | Class Setup | Use this screen to set up the bandwidth classes. |
| | Monitor | Use this screen to view the ZyWALL's bandwidth usage and allotments. |
| DNS | System | Use this screen to configure the address and name server records. |
| | Cache | Use this screen to configure the DNS resolution cache. |
| | DHCP | Use this screen to configure LAN/DMZ/WLAN DNS information. |
| | DDNS | Use this screen to set up dynamic DNS. |
| REMOTE MGMT | WWW | Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or HTTP to manage the ZyWALL. |
| | SSH | Use this screen to configure through which interface(s) and from which IP address(es) users can use Secure Shell to manage the ZyWALL. |
| | TELNET | Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyWALL. |
| | FTP | Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyWALL. |
| | SNMP | Use this screen to configure your ZyWALL's settings for Simple Network Management Protocol management. |
| | DNS | Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyWALL. |
| | CNM | Use this screen to configure and allow your ZyWALL to be managed by the Vantage CNM server. |
| UPnP | UPnP | Use this screen to enable UPnP on the ZyWALL. |
| | Ports | Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL. |
| Custom APP | Custom APP | Use this screen to specify port numbers for the ZyWALL to monitor for FTP, HTTP, SMTP, POP3, H323, and SIP traffic. |
| ALG | ALG | Use this screen to allow certain applications to pass through the ZyWALL. |

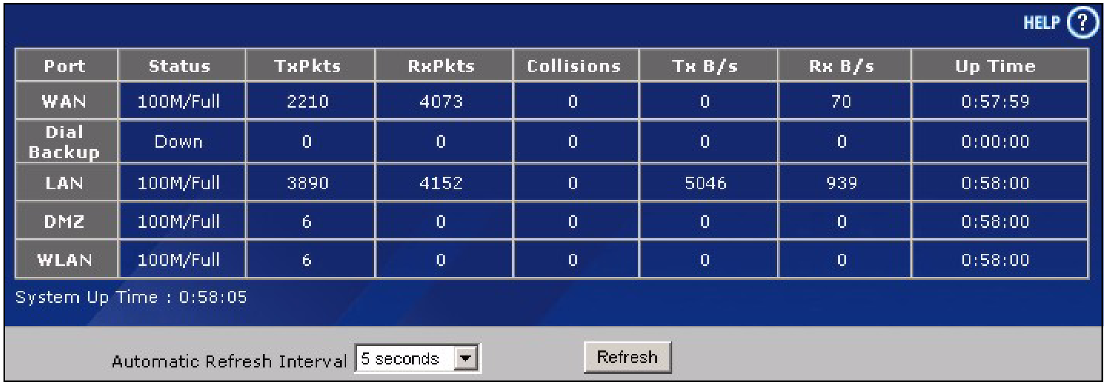
**Table 6** Screens Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| LOGS | View Log | Use this screen to view the logs for the categories that you selected. |
| | Log Settings | Use this screen to change your ZyWALL’s log settings. |
| | Reports | Use this screen to have the ZyWALL record and display network usage reports. |
| MAINTENANCE | General | This screen contains administrative. |
| | Password | Use this screen to change your password. |
| | Time and Date | Use this screen to change your ZyWALL’s time and date. |
| | Device Mode | Use this screen to configure and have your ZyWALL work as a router or a bridge. |
| | F/W Upload | Use this screen to upload firmware to your ZyWALL |
| | Backup & Restore | Use this screen to backup and restore the configuration or reset the factory defaults to your ZyWALL. |
| | Restart | This screen allows you to reboot the ZyWALL without turning the power off. |
| | Diagnosis | Use this screen to have the ZyWALL generate and send diagnostic files by e-mail and/or the console port. |
| LOGOUT | | Click this label to exit the web configurator. |

## 2.4.6 Port Statistics

Click **Port Statistics** in the **HOME** screen. Read-only information here includes port status and packet specific statistics. The **Poll Interval(s)** field is configurable.

**Figure 10** HOME > Show Statistics



| Port | Status | TxPkts | RxPkts | Collisions | Tx B/s | Rx B/s | Up Time |
|---|---|---|---|---|---|---|---|
| WAN | 100M/Full | 2210 | 4073 | 0 | 0 | 70 | 0:57:59 |
| Dial Backup | Down | 0 | 0 | 0 | 0 | 0 | 0:00:00 |
| LAN | 100M/Full | 3890 | 4152 | 0 | 5046 | 939 | 0:58:00 |
| DMZ | 100M/Full | 6 | 0 | 0 | 0 | 0 | 0:58:00 |
| WLAN | 100M/Full | 6 | 0 | 0 | 0 | 0 | 0:58:00 |

System Up Time : 0:58:05

Automatic Refresh Interval: 5 seconds

The following table describes the labels in this screen.

**Table 7** HOME > Show Statistics

| LABEL | DESCRIPTION |
|---|---|
| Port | These are the ZyWALL’s interfaces. |
| Status | For the WAN and dial backup ports, this displays the port speed and duplex setting if you’re using Ethernet encapsulation and **Down** (line is down), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you’re using PPPoE encapsulation. Dial backup is not available in bridge mode.<br>For the LAN, DMZ and WLAN ports, this displays the port speed and duplex setting. |

**Table 7** HOME > Show Statistics (continued)

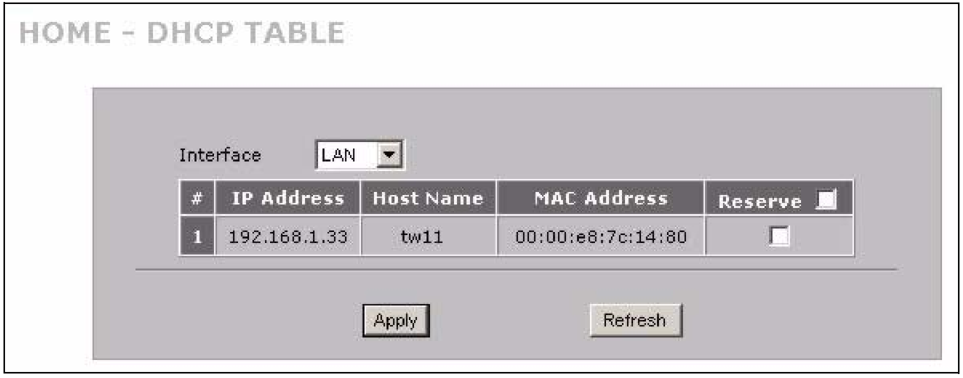
| LABEL | DESCRIPTION |
|---|---|
| TxPkts | This is the number of transmitted packets on this port. |
| RxPkts | This is the number of received packets on this port. |
| Collisions | This is the number of collisions on this port. |
| Tx B/s | This displays the transmission speed in bytes per second on this port. |
| Rx B/s | This displays the reception speed in bytes per second on this port. |
| Up Time | This is the total amount of time the line has been up. |
| System Up Time | This is the total time the ZyWALL has been on. |
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |

## 2.4.7 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyWALL as a DHCP server or disable it. When configured as a server, the ZyWALL provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Show DHCP Table** in the **HOME** screen when the ZyWALL is set to router mode. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyWALL's DHCP server.

**Figure 11** HOME > DHCP Table



HOME - DHCP TABLE

Interface: LAN

| # | IP Address | Host Name | MAC Address | Reserve ☐ |
|---|---|---|---|---|
| 1 | 192.168.1.33 | tw11 | 00:00:e8:7c:14:80 | ☐ |

The following table describes the labels in this screen.

**Table 8** HOME > DHCP Table

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select **LAN**, **DMZ** or **WLAN** to show the current DHCP client information for the specified interface. |
| # | This is the index number of the host computer. |
| IP Address | This field displays the IP address relative to the # field listed above. |
| Host Name | This field displays the computer host name. |

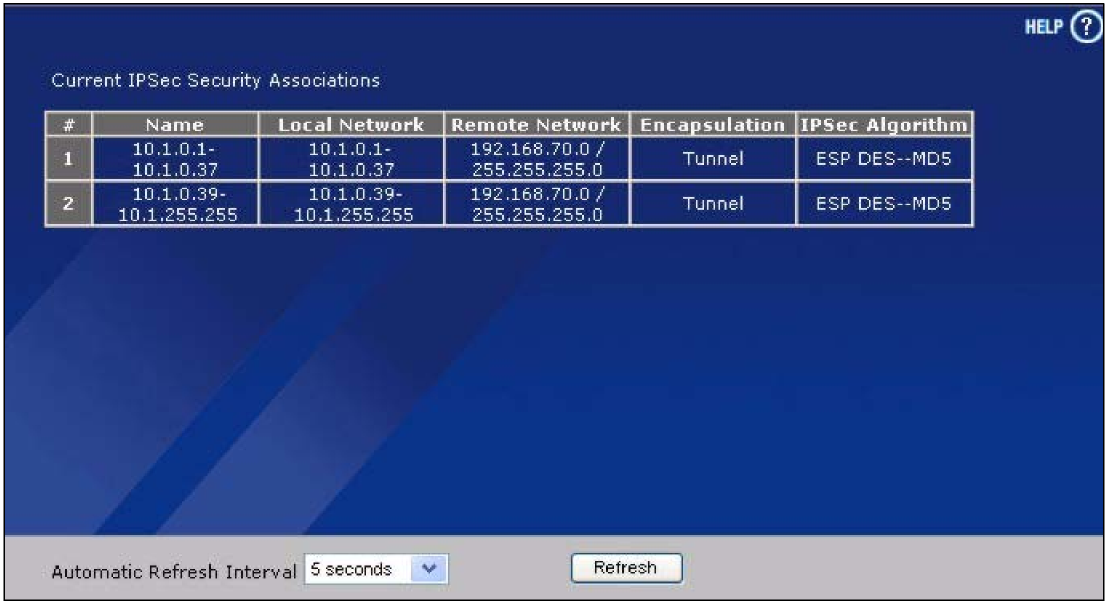
**Table 8** HOME > DHCP Table (continued)

| LABEL | DESCRIPTION |
|---|---|
| MAC Address | The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).<br>A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address. |
| Reserve | Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyWALL always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 32 entries in this table. After you click **Apply**, the MAC address and IP address also display in the **Static DHCP** screen (where you can edit them) for the specified interface. |
| Refresh | Click **Refresh** to reload the DHCP table. |

## 2.4.8 VPN Status

Click **VPN** in the **HOME** screen when the ZyWALL is set to router mode. This screen displays read-only information about the active VPN connections. The **Poll Interval(s)** field is configurable. A Security Association (SA) is the group of security settings related to a specific VPN tunnel.

**Figure 12** HOME > VPN Status



Current IPSec Security Associations

| # | Name | Local Network | Remote Network | Encapsulation | IPSec Algorithm |
|---|---|---|---|---|---|
| 1 | 10.1.0.1-<br>10.1.0.37 | 10.1.0.1-<br>10.1.0.37 | 192.168.70.0 /<br>255.255.255.0 | Tunnel | ESP DES--MD5 |
| 2 | 10.1.0.39-<br>10.1.255.255 | 10.1.0.39-<br>10.1.255.255 | 192.168.70.0 /<br>255.255.255.0 | Tunnel | ESP DES--MD5 |

Automatic Refresh Interval 5 seconds

The following table describes the labels in this screen.

**Table 9** HOME > VPN Status

| LABEL | DESCRIPTION |
|---|---|
| # | This is the security association index number. |
| Name | This field displays the identification name for this VPN policy. |
| Local Network | This field displays the IP address of the computer using the VPN IPSec feature of your ZyWALL. |
| Remote Network | This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router. |

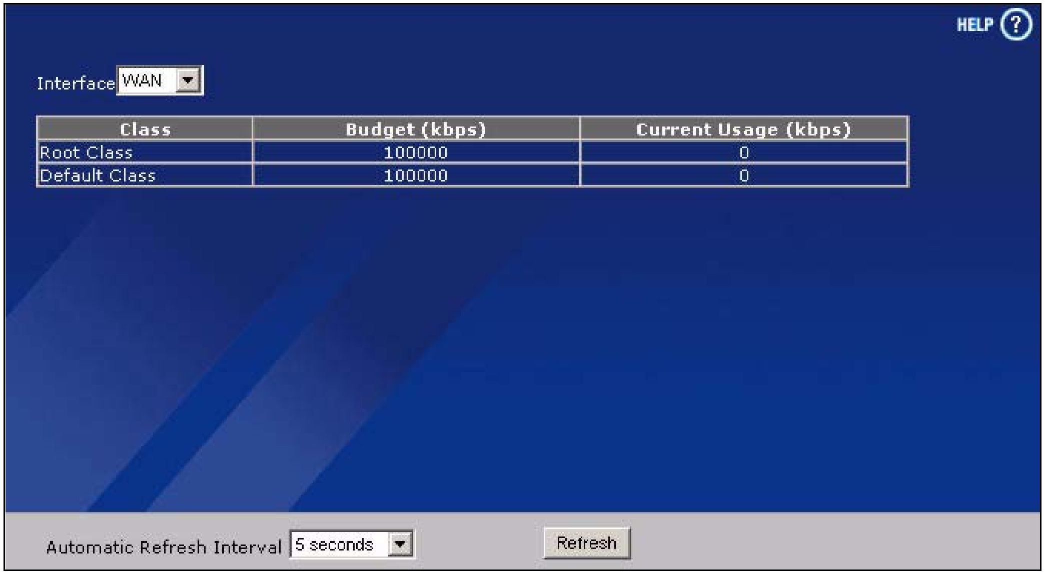
**Table 9** HOME > VPN Status

| LABEL | DESCRIPTION |
|---|---|
| Encapsulation | This field displays **Tunnel** or **Transport** mode. |
| IPSec Algorithm | This field displays the security protocols used for an SA.<br>Both AH and ESP increase ZyWALL processing requirements and communications latency (delay). |
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |

## 2.4.9 Bandwidth Monitor

Click **Bandwidth** in the **HOME** screen to display the bandwidth monitor. This screen displays the device's bandwidth usage and allotments.

**Figure 13** Home > Bandwidth Monitor



Interface WAN

| Class | Budget (kbps) | Current Usage (kbps) |
|---|---|---|
| Root Class | 100000 | 0 |
| Default Class | 100000 | 0 |

Automatic Refresh Interval 5 seconds

The following table describes the labels in this screen.

**Table 10** ADVANCED > BW MGMT > Monitor

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes. |
| Class | This field displays the name of the bandwidth class.<br>A **Default Class** automatically displays for all the bandwidth in the **Root Class** that is not allocated to bandwidth classes. If you do not enable maximize bandwidth usage on an interface, the ZyWALL uses the bandwidth in this default class to send traffic that does not match any of the bandwidth classes.[A] |
| Budget (kbps) | This field displays the amount of bandwidth allocated to the bandwidth class. |
| Current Usage (kbps) | This field displays the amount of bandwidth that each bandwidth class is using. |

**Table 10** ADVANCED > BW MGMT > Monitor

| LABEL | DESCRIPTION |
|---|---|
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |

A.If you allocate all the root class's bandwidth to the bandwidth classes, the default class still displays a budget of 2 kbps (the minimum amount of bandwidth that can be assigned to a bandwidth class).

# 3

# Wizard Setup

This chapter provides information on the **Wizard Setup** screens in the web configurator. The Internet access wizard is only applicable when the ZyWALL is in router mode.

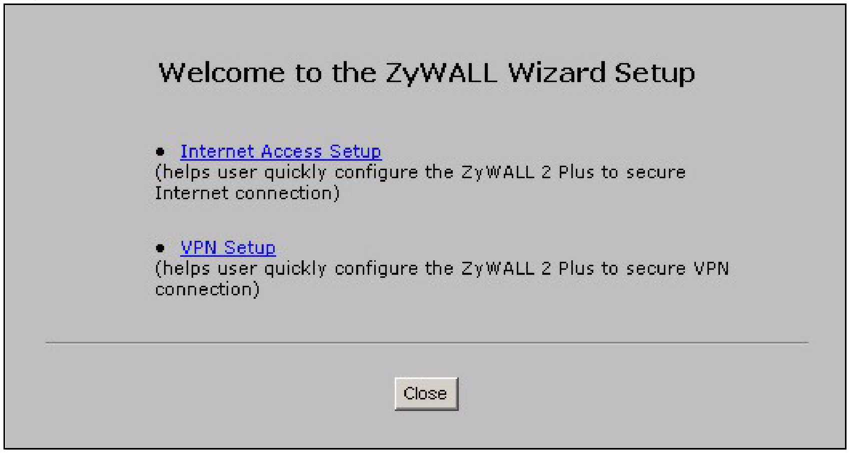
## 3.1 Wizard Setup Overview

The web configurator's setup wizards help you configure Internet and VPN connection settings.

In the **HOME** screen, click the wizard icon WIZARD to open the **Wizard Setup Welcome** screen. The following summarizes the wizards you can select:

- **Internet Access Setup**
  Click this link to open a wizard to set up an Internet connection for the WAN port on the ZyWALL (in router mode).
- **VPN Setup**
  Use **VPN Setup** to configure a VPN connection that uses a pre-shared key. If you want to set the rule to use a certificate, please go to the VPN screens for configuration. See Section 3.3 on page 79.

**Figure 14** Wizard Setup Welcome



Welcome to the ZyWALL Wizard Setup

- Internet Access Setup
(helps user quickly configure the ZyWALL 2 Plus to secure Internet connection)

- VPN Setup
(helps user quickly configure the ZyWALL 2 Plus to secure VPN connection)

## 3.2 Internet Access

The Internet access wizard screen has three variations depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

### 3.2.1 ISP Parameters

The ZyWALL offers three choices of encapsulation. They are **Ethernet**, **PPTP** or **PPPoE**.

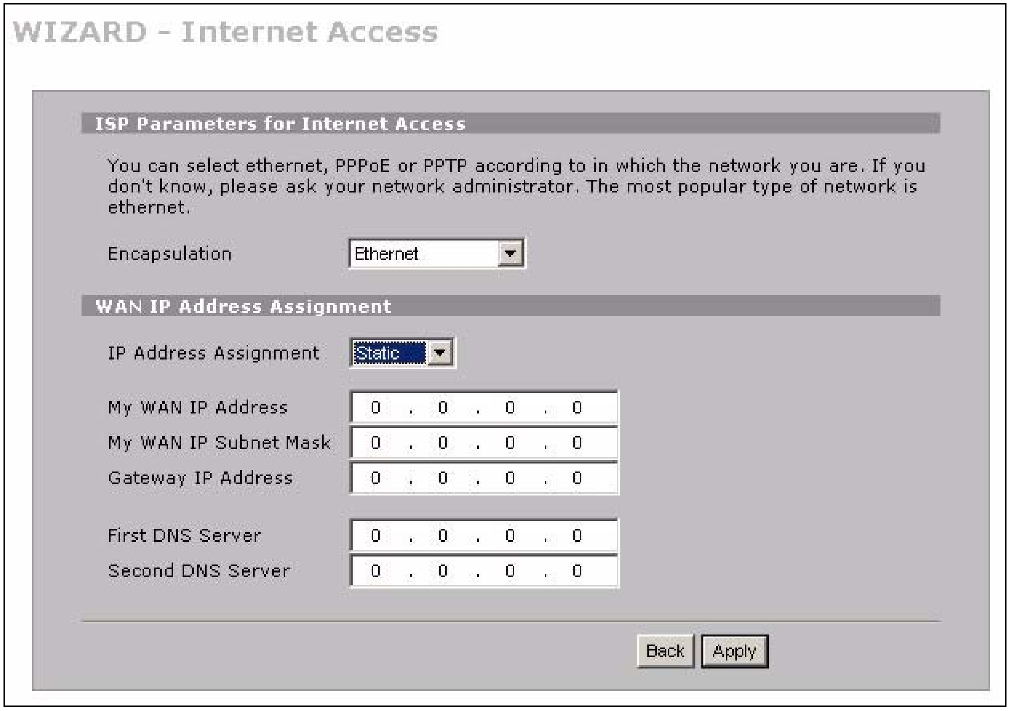
The wizard screen varies according to the type of encapsulation that you select in the **Encapsulation** field.

#### 3.2.1.1 Ethernet

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/ZyWALL** firewall rule for those packets. Contact your ISP to find the correct port number.

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

**Figure 15** ISP Parameters: Ethernet Encapsulation



WIZARD - Internet Access

ISP Parameters for Internet Access

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation: Ethernet

WAN IP Address Assignment

IP Address Assignment: Static

My WAN IP Address: 0 . 0 . 0 . 0
My WAN IP Subnet Mask: 0 . 0 . 0 . 0
Gateway IP Address: 0 . 0 . 0 . 0

First DNS Server: 0 . 0 . 0 . 0
Second DNS Server: 0 . 0 . 0 . 0

The following table describes the labels in this screen.

**Table 11** ISP Parameters: Ethernet Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection. |

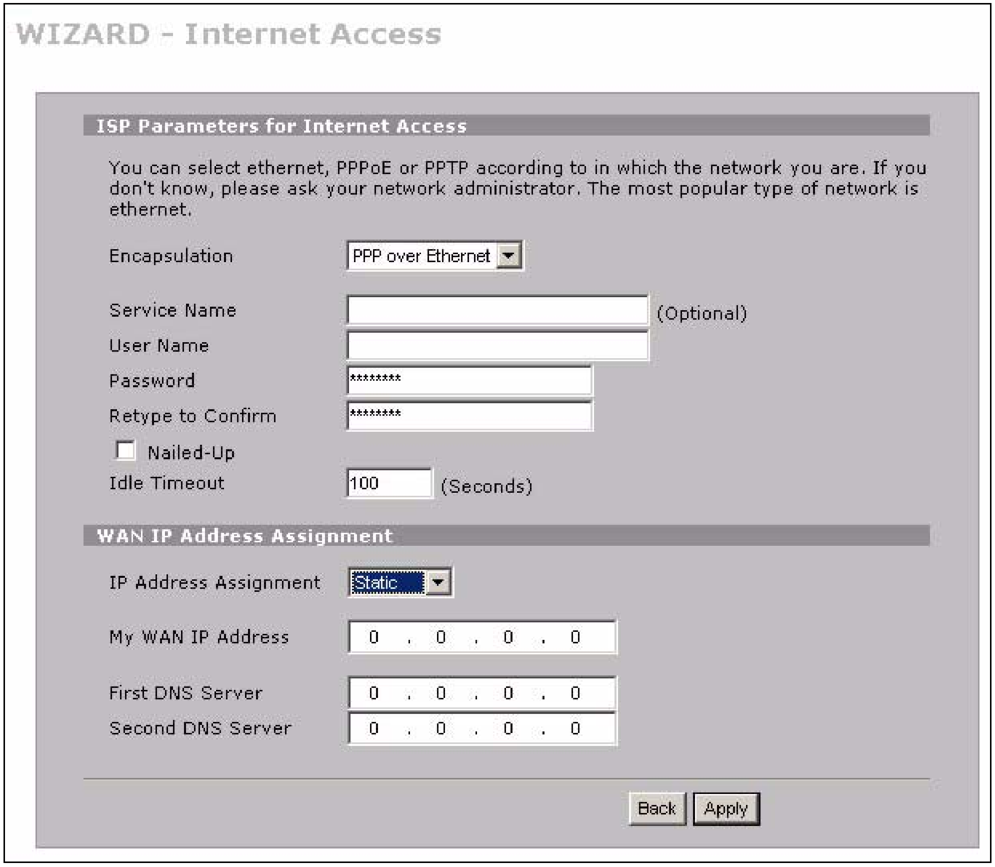
**Table 11** ISP Parameters: Ethernet Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| WAN IP Address Assignment | |
| IP Address Assignment | Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection.<br>Select **Static** If the ISP assigned a fixed IP address.<br>The fields below are available only when you select **Static**. |
| My WAN IP Address | Enter your WAN IP address in this field. |
| My WAN IP Subnet Mask | Enter the IP subnet mask in this field. |
| Gateway IP Address | Enter the gateway IP address in this field. |
| First DNS Server<br>Second DNS Server | Enter the DNS server's IP address(es) in the field(s) to the right.<br>Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. |
| Back | Click **Back** to return to the previous wizard screen. |
| Apply | Click **Apply** to save your changes and go to the next screen. |

#### 3.2.1.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

**Figure 16**   ISP Parameters: PPPoE Encapsulation



You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation: PPP over Ethernet

Service Name: (Optional)

User Name:

Password: ********

Retype to Confirm: ********

☐ Nailed-Up

Idle Timeout: 100 (Seconds)

IP Address Assignment: Static

My WAN IP Address: 0 . 0 . 0 . 0

First DNS Server: 0 . 0 . 0 . 0

Second DNS Server: 0 . 0 . 0 . 0

The following table describes the labels in this screen.

**Table 12**   ISP Parameters: PPPoE Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameter for Internet Access | |
| Encapsulation | Choose an encapsulation method from the pull-down list box. **PPP over Ethernet** forms a dial-up connection. |
| Service Name | Type the name of your service provider. This field is optional. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to Confirm | Type your password again for confirmation. |
| Nailed-Up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds. |
| WAN IP Address Assignment | |
| IP Address Assignment | Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection.<br>Select **Static** If the ISP assigned a fixed IP address.<br>The fields below are available only when you select **Static**. |

**Table 12** ISP Parameters: PPPoE Encapsulation (continued)

| LABEL | DESCRIPTION |
|---|---|
| My WAN IP Address | Enter your WAN IP address in this field. |
| First DNS Server<br>Second DNS Server | Enter the DNS server's IP address(es) in the field(s) to the right.<br>Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. |
| Back | Click **Back** to return to the previous wizard screen. |
| Apply | Click **Apply** to save your changes and go to the next screen. |

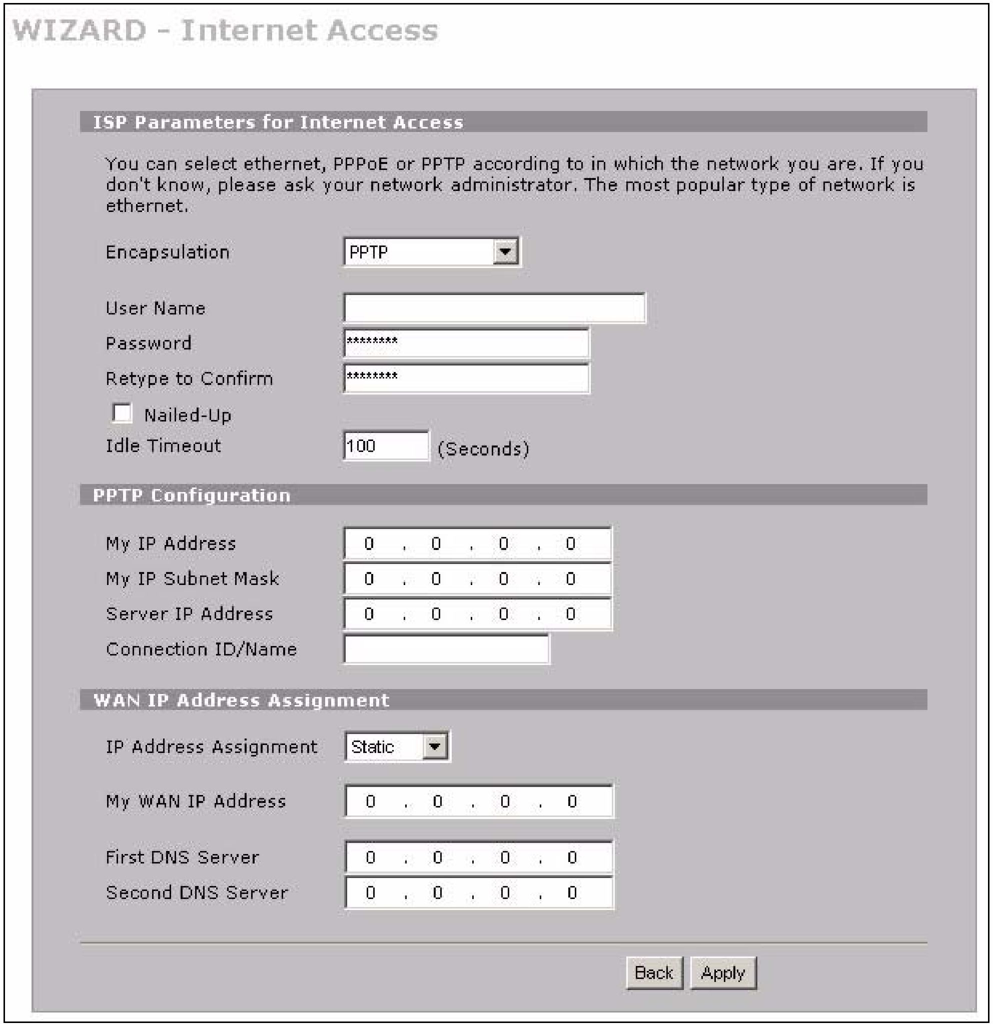
#### 3.2.1.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

The ZyWALL supports one PPTP server connection at any given time.

**Figure 17** ISP Parameters: PPTP Encapsulation



You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation: PPTP
User Name:
Password: ********
Retype to Confirm: ********
☐ Nailed-Up
Idle Timeout: 100 (Seconds)
My IP Address: 0 . 0 . 0 . 0
My IP Subnet Mask: 0 . 0 . 0 . 0
Server IP Address: 0 . 0 . 0 . 0
Connection ID/Name:
IP Address Assignment: Static
My WAN IP Address: 0 . 0 . 0 . 0
First DNS Server: 0 . 0 . 0 . 0
Second DNS Server: 0 . 0 . 0 . 0

The following table describes the labels in this screen.

**Table 13** ISP Parameters: PPTP Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | Select **PPTP** from the drop-down list box. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the User Name above. |
| Retype to Confirm | Type your password again for confirmation. |
| Nailed-Up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. |
| PPTP Configuration | |
| My IP Address | Type the (static) IP address assigned to you by your ISP. |

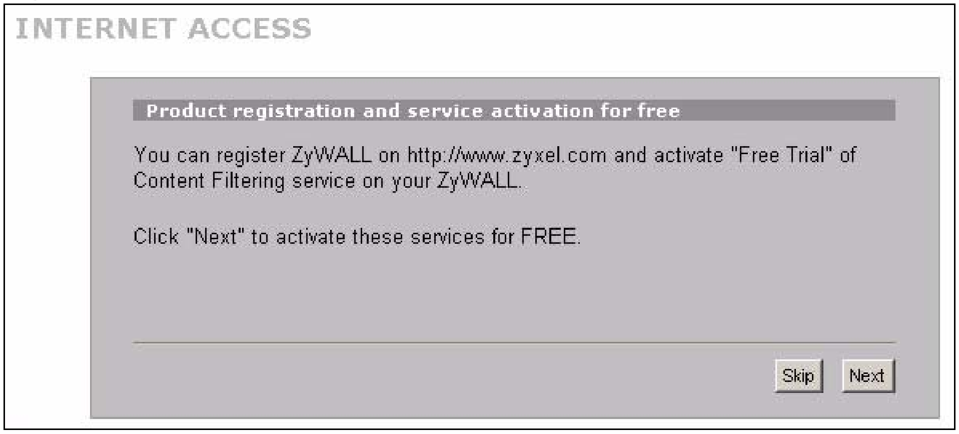
**Table 13** ISP Parameters: PPTP Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| My IP Subnet Mask | Type the subnet mask assigned to you by your ISP (if given). |
| Server IP Address | Type the IP address of the PPTP server. |
| Connection ID/ Name | Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP.<br>This field is optional and depends on the requirements of your xDSL modem. |
| WAN IP Address Assignment | |
| IP Address Assignment | Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection.<br>Select **Static** If the ISP assigned a fixed IP address.<br>The fields below are available only when you select **Static**. |
| My WAN IP Address | Enter your WAN IP address in this field. |
| First DNS Server<br>Second DNS Server | Enter the DNS server's IP address(es) in the field(s) to the right.<br>Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. |
| Back | Click **Back** to return to the previous wizard screen. |
| Apply | Click **Apply** to save your changes and go to the next screen. |

## 3.2.2 Internet Access Wizard: Second Screen

Click **Next** to go to the screen where you can register your ZyWALL and activate the free content filtering trial application. Otherwise, click **Skip** to display the congratulations screen and click **Close** to complete the Internet access setup.

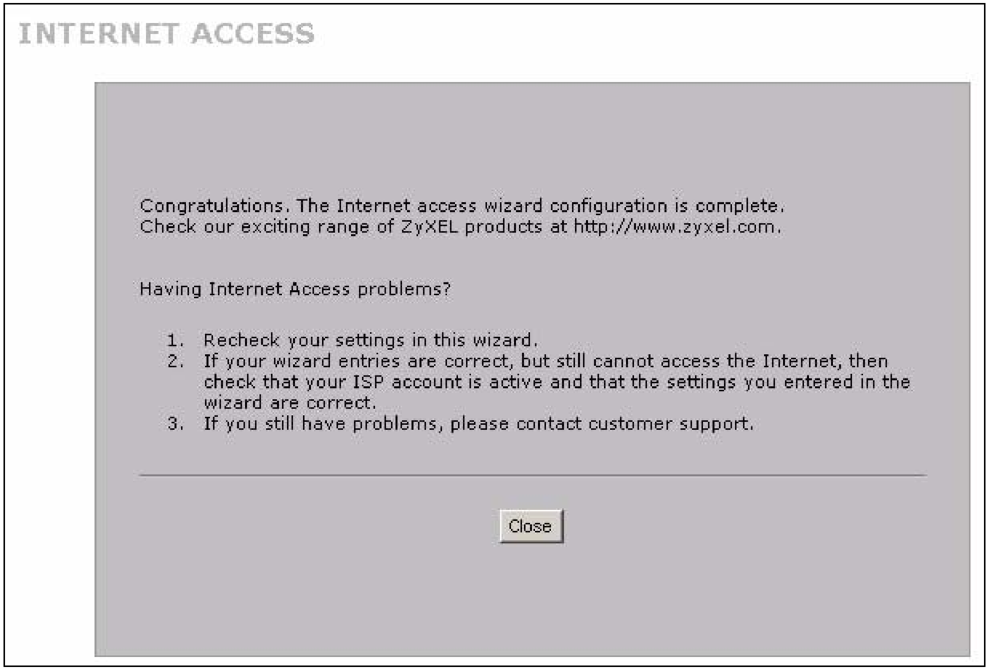
**Figure 18** Internet Access Wizard: Second Screen



You can register ZyWALL on http://www.zyxel.com and activate "Free Trial" of Content Filtering service on your ZyWALL.

Click "Next" to activate these services for FREE.

**Figure 19** Internet Access Setup Complete



Congratulations. The Internet access wizard configuration is complete.
Check our exciting range of ZyXEL products at http://www.zyxel.com.

Having Internet Access problems?

1. Recheck your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

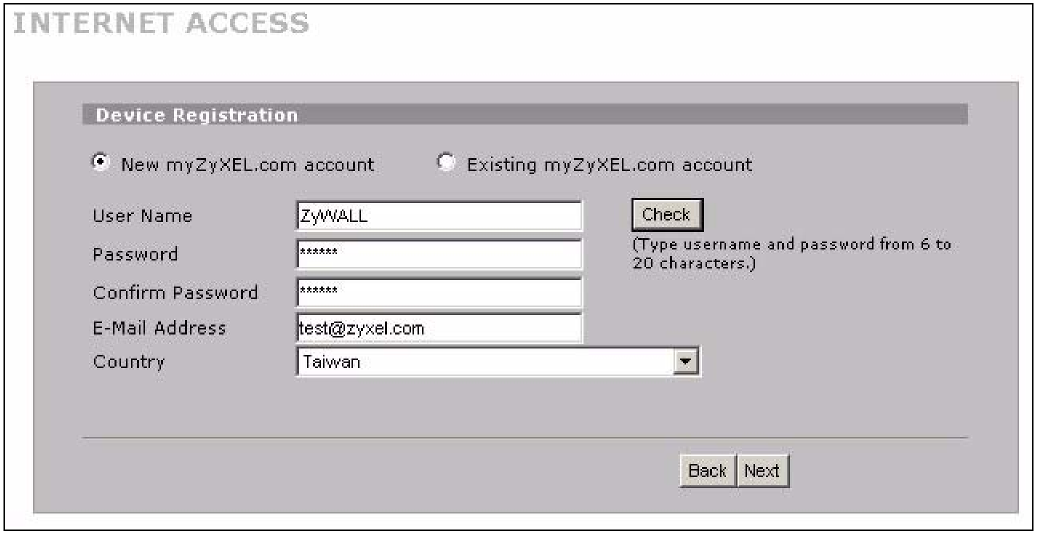
## 3.2.3 Internet Access Wizard: Registration

If you clicked **Next** in the previous screen (see Figure 18 on page 75), the following screen displays.

Use this screen to register the ZyWALL with myZyXEL.com. You must register your ZyWALL before you can activate trial application of service like content filtering.

If you want to activate a standard service with your iCard's PIN number (license key), use the **REGISTRATION > Service** screen.

**Figure 20** Internet Access Wizard: Registration



● New myZyXEL.com account ○ Existing myZyXEL.com account

User Name: ZyWALL

Password: ******

Confirm Password: ******

(Type username and password from 6 to 20 characters.)

E-Mail Address: test@zyxel.com

Country: Taiwan

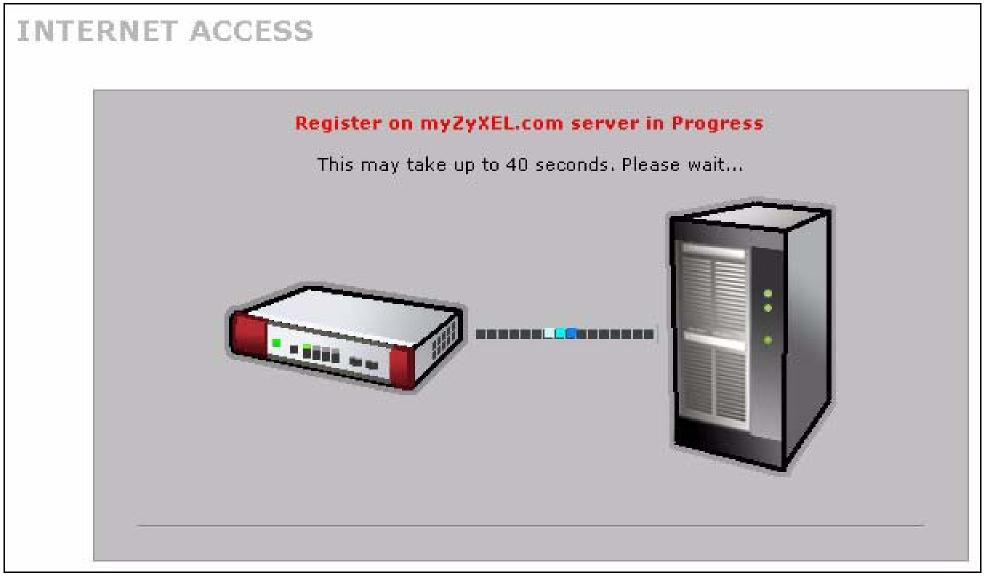
The following table describes the labels in this screen.

**Table 14** Internet Access Wizard: Registration

| LABEL | DESCRIPTION |
|---|---|
| Device Registration | If you select **Existing myZyXEL.com account**, only the **User Name** and **Password** fields are available. |
| New myZyXEL.com account | If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL. |
| Existing myZyXEL.com account | If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL. |
| User Name | Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Check | Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used. |
| Password | Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Confirm Password | Enter the password again for confirmation. |
| E-Mail Address | Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces. |
| Country | Select your country from the drop-down box list. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

After you fill in the fields and click **Next**, the following screen shows indicating the registration is in progress. Wait for the registration progress to finish.

**Figure 21** Internet Access Wizard: Registration in Progress



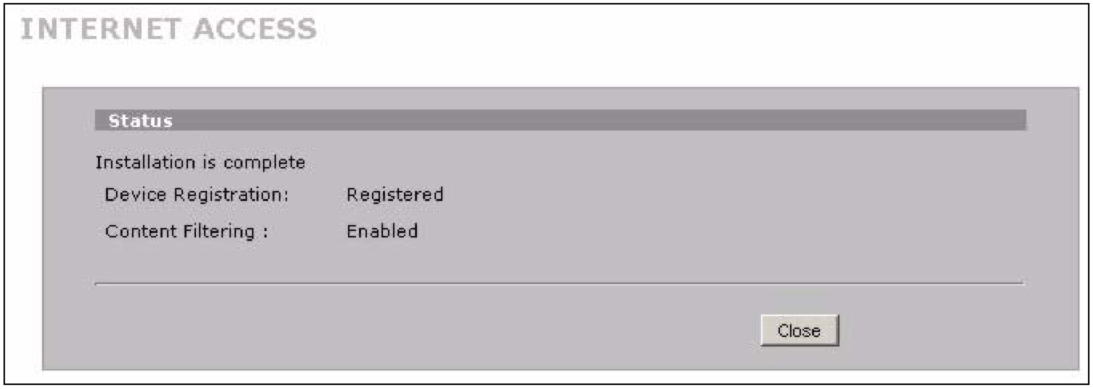
INTERNET ACCESS

Register on myZyXEL.com server in Progress

This may take up to 40 seconds. Please wait...

Click **Close** to leave the wizard screen when the registration and activation are done.

**Figure 22** Internet Access Wizard: Status



INTERNET ACCESS

Status

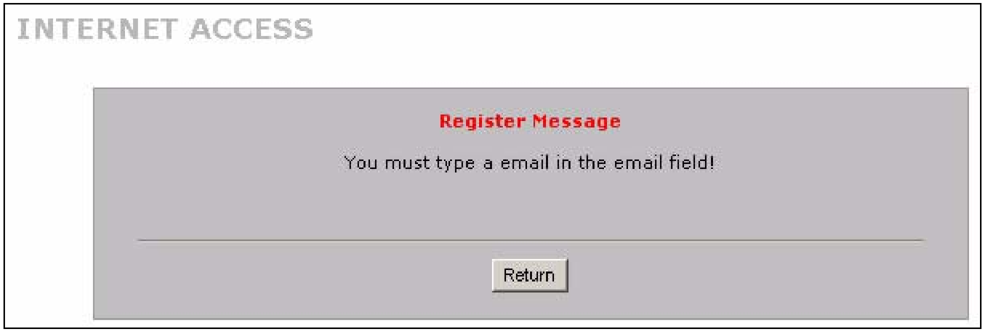
Installation is complete

Device Registration: Registered

Content Filtering : Enabled

The following screen appears if the registration was not successful. Click **Return** to go back to the **Device Registration** screen and check your settings.

**Figure 23** Internet Access Wizard: Registration Failed



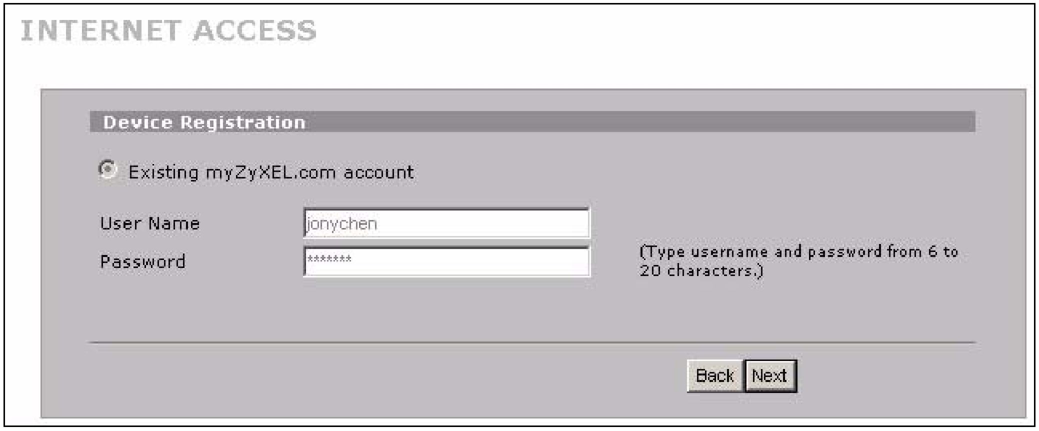
INTERNET ACCESS

Register Message

You must type a email in the email field!

If the ZyWALL has been registered, the **Device Registration** screen is read-only and the **Service Activation** screen appears indicating what trial applications are activated after you click **Next**.

**Figure 24** Internet Access Wizard: Registered Device


INTERNET ACCESS
Device Registration
Back
Next

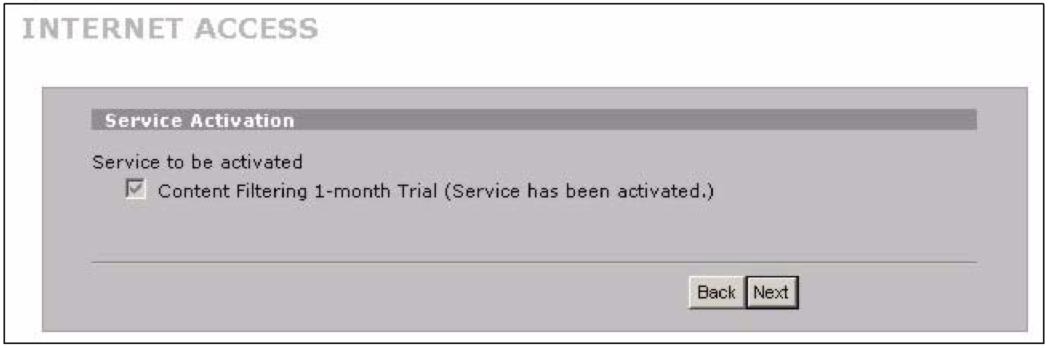
● Existing myZyXEL.com account

User Name: jonychen

Password: *******

(Type username and password from 6 to 20 characters.)

**Figure 25** Internet Access Wizard: Activated Services


INTERNET ACCESS
Service Activation
Back
Next

Service to be activated

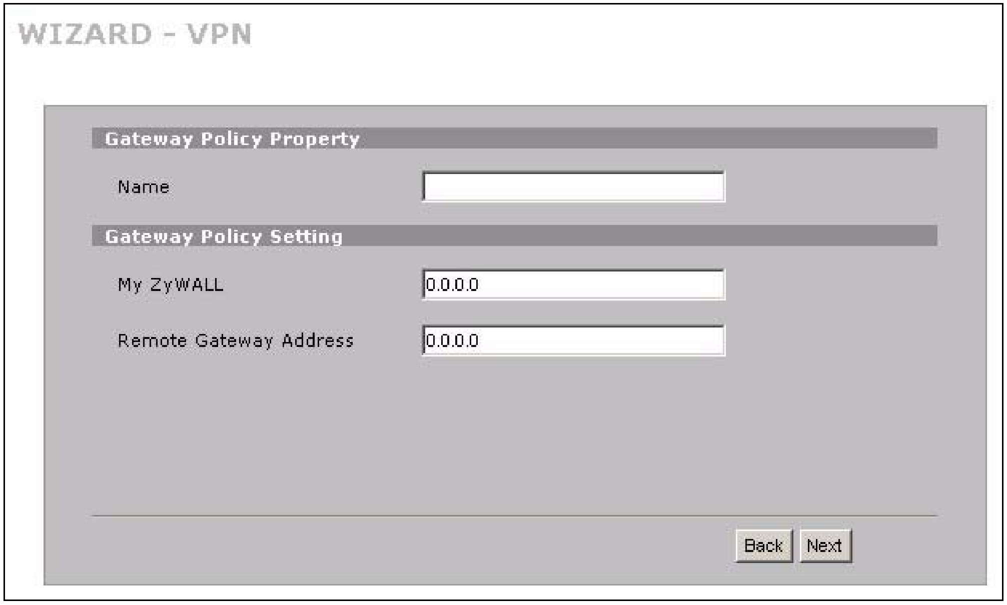
☑ Content Filtering 1-month Trial (Service has been activated.)

## 3.3 VPN Wizard Gateway Setting

Use this screen to name the VPN gateway policy (IKE SA) and identify the IPSec routers at either end of the VPN tunnel.

Click **VPN Setup** in the **Wizard Setup Welcome** screen (Figure 14 on page 69) to open the VPN configuration wizard. The first screen displays as shown next.

**Figure 26** VPN Wizard: Gateway Setting



Name

My ZyWALL: 0.0.0.0

Remote Gateway Address: 0.0.0.0

The following table describes the labels in this screen.

**Table 15** VPN Wizard: Gateway Setting

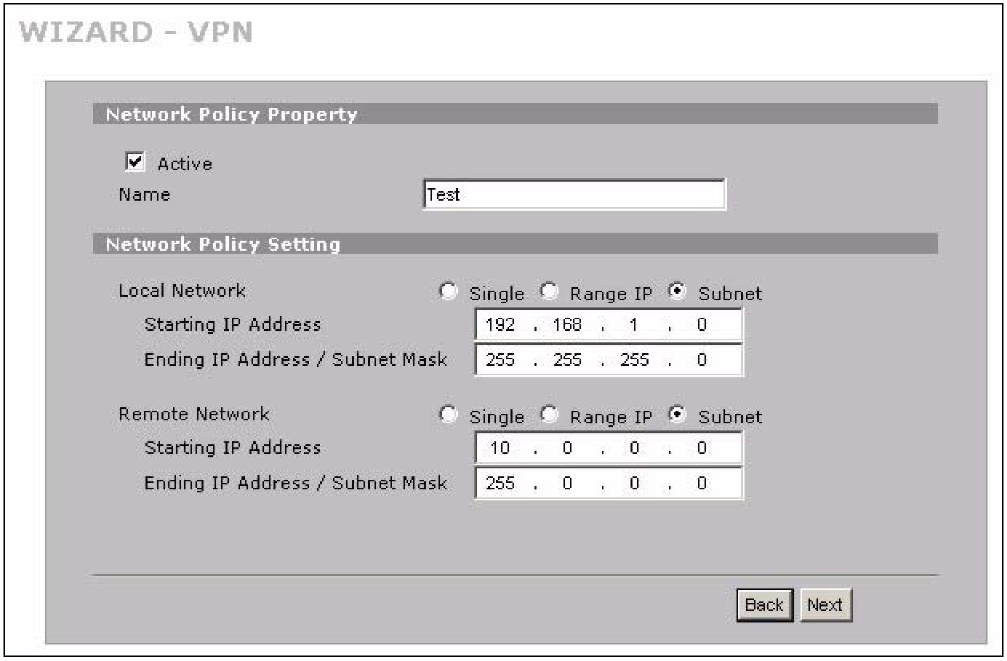
| LABEL | DESCRIPTION |
|---|---|
| Gateway Policy Property | |
| Name | Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Gateway Policy Setting | |
| My ZyWALL | When the ZyWALL is in router mode, enter the WAN IP address or the domain name of your ZyWALL or leave the field set to **0.0.0.0**.<br>The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.<br>The VPN tunnel has to be rebuilt if this IP address changes.<br>When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address. |
| Remote Gateway Address | Enter the WAN IP address or domain name of the remote IPSec router (secure gateway) in the field below to identify the remote IPSec router by its IP address or a domain name. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 3.4 VPN Wizard Network Setting

Use this screen to name the VPN network policy (IPSec SA) and identify the devices behind the IPSec routers at either end of a VPN tunnel.

Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.

**Figure 27** VPN Wizard: Network Setting



WIZARD - VPN

Network Policy Property

☑ Active

Name: Test

Network Policy Setting

Local Network: ○ Single ○ Range IP ● Subnet

Starting IP Address: 192 . 168 . 1 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Remote Network: ○ Single ○ Range IP ● Subnet

Starting IP Address: 10 . 0 . 0 . 0

Ending IP Address / Subnet Mask: 255 . 0 . 0 . 0

The following table describes the labels in this screen.

**Table 16** VPN Wizard: Network Setting

| LABEL | DESCRIPTION |
|---|---|
| Network Policy Property | |
| Active | If the **Active** check box is selected, packets for the tunnel trigger the ZyWALL to build the tunnel.<br>Clear the **Active** check box to turn the network policy off. The ZyWALL does not apply the policy. Packets for the tunnel do not trigger the tunnel. |
| Name | Type up to 32 characters to identify this VPN network policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Network Policy Setting | |
| Local Network | Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.<br>Select **Single** for a single IP address. Select **Range IP** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Local Network** field is configured to **Single**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Local Network** field is configured to **Range IP**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Local Network** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your ZyWALL. |
| Ending IP Address/ Subnet Mask | When the **Local Network** field is configured to **Single**, this field is N/A. When the **Local Network** field is configured to **Range IP**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Local Network** field is configured to **Subnet**, this is a subnet mask on the LAN behind your ZyWALL. |

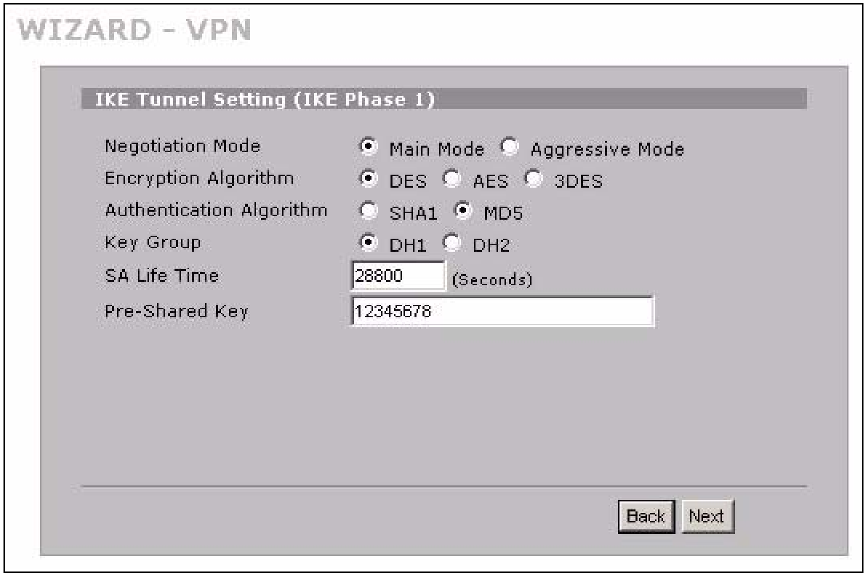
**Table 16** VPN Wizard: Network Setting

| LABEL | DESCRIPTION |
|---|---|
| Remote Network | Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses.<br>Select **Single** for a single IP address. Select **Range IP** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Remote Network** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Range IP**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router |
| Ending IP Address/ Subnet Mask | When the **Remote Network** field is configured to **Single**, this field is N/A. When the **Remote Network** field is configured to **Range IP**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 3.5 VPN Wizard IKE Tunnel Setting (IKE Phase 1)

Use this screen to specify the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

**Figure 28** VPN Wizard: IKE Tunnel Setting



Negotiation Mode ● Main Mode ○ Aggressive Mode
Encryption Algorithm ● DES ○ AES ○ 3DES
Authentication Algorithm ○ SHA1 ● MD5
Key Group ● DH1 ○ DH2
SA Life Time 28800 (Seconds)
Pre-Shared Key 12345678

The following table describes the labels in this screen.

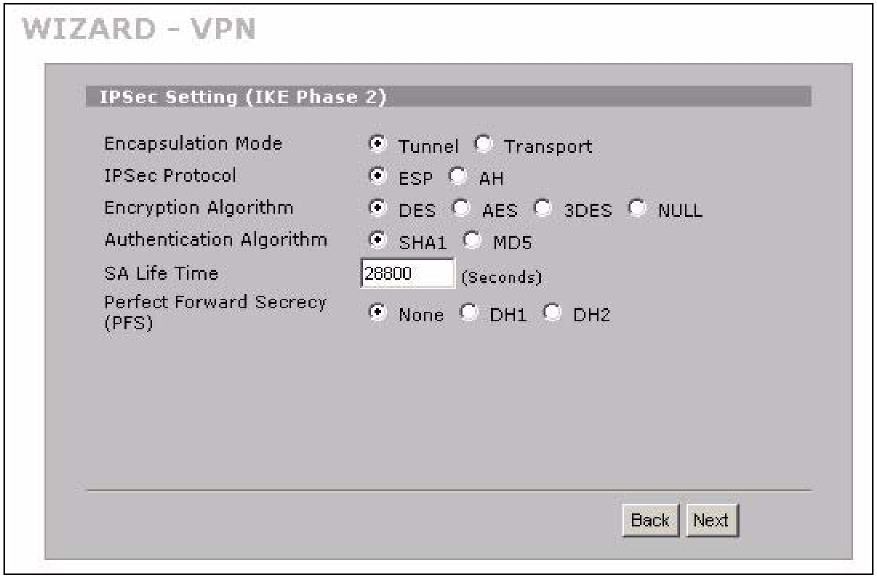
**Table 17** VPN Wizard: IKE Tunnel Setting

| LABEL | DESCRIPTION |
|---|---|
| Negotiation Mode | Select **Main Mode** for identity protection. Select **Aggressive Mode** to allow more incoming connections from dynamic IP addresses to use separate passwords.<br>Note: Multiple SAs (security associations) connecting through a secure gateway must have the same negotiation mode. |
| Encryption Algorithm | When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. |
| Authentication Algorithm | **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security. |
| Key Group | You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. |
| SA Life Time (Seconds) | Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds.<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Pre-Shared Key | Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.<br>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself.<br>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 3.6 VPN Wizard IPSec Setting (IKE Phase 2)

Use this screen to specify the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

**Figure 29** VPN Wizard: IPSec Setting



Encapsulation Mode ● Tunnel ○ Transport
IPSec Protocol ● ESP ○ AH
Encryption Algorithm ● DES ○ AES ○ 3DES ○ NULL
Authentication Algorithm ● SHA1 ○ MD5
SA Life Time 28800 (Seconds)
Perfect Forward Secrecy (PFS) ● None ○ DH1 ○ DH2

The following table describes the labels in this screen.

**Table 18** VPN Wizard: IPSec Setting

| LABEL | DESCRIPTION |
|---|---|
| Encapsulation Mode | **Tunnel** is compatible with NAT, **Transport** is not.<br>Tunnel mode encapsulates the entire IP packet to transmit it securely. A Tunnel mode is required for gateway services to provide access to internal systems. Tunnel mode is fundamentally an IP tunnel with authentication and encryption. Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In Transport mode, the IP packet contains the security protocol (AH or ESP) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP). |
| IPSec Protocol | Select the security protocols used for an SA.<br>Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay). |
| Encryption Algorithm | When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key. |
| Authentication Algorithm | **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security. |
| SA Life Time (Seconds) | Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds.<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |

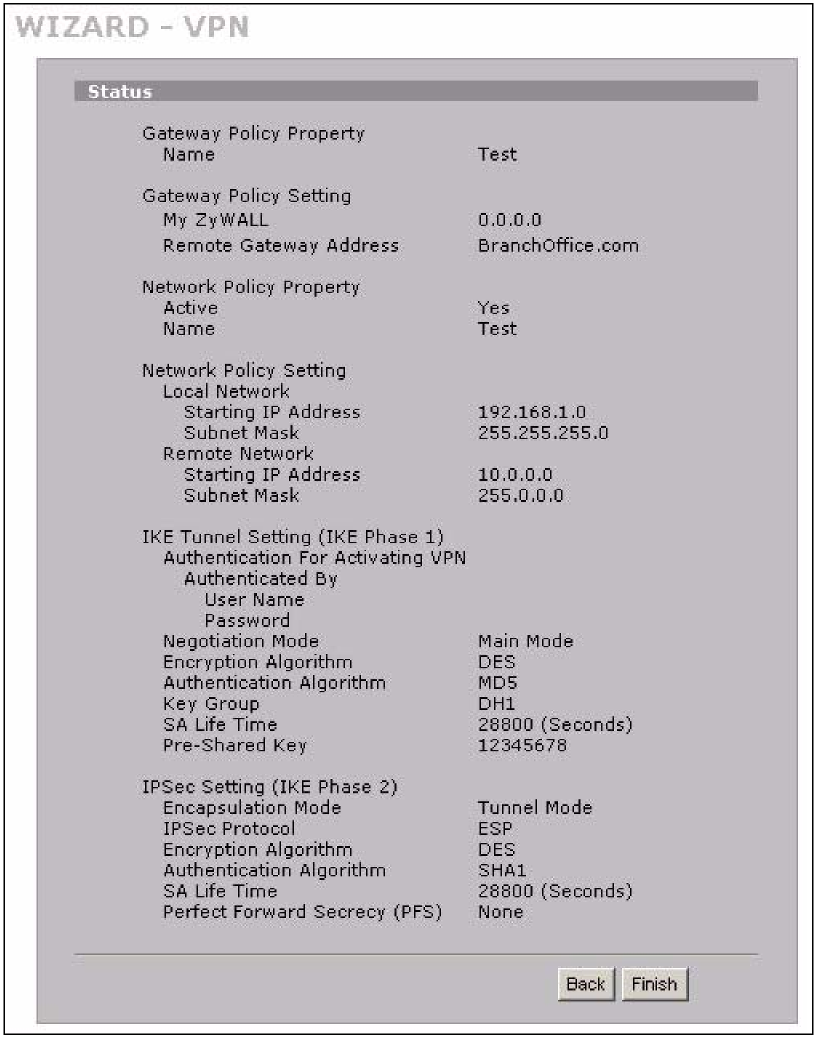
**Table 18** VPN Wizard: IPSec Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| Perfect Forward Secret (PFS) | Perfect Forward Secret (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure.<br>Select **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower). |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 3.7 VPN Wizard Status Summary

This read-only screen shows the status of the current VPN setting. Use the summary table to check whether what you have configured is correct.

**Figure 30** VPN Wizard: VPN Status



```
WIZARD - VPN

Status

Gateway Policy Property
  Name                               Test

Gateway Policy Setting
  My ZyWALL                          0.0.0.0
  Remote Gateway Address             BranchOffice.com

Network Policy Property
  Active                             Yes
  Name                               Test

Network Policy Setting
  Local Network
    Starting IP Address              192.168.1.0
    Subnet Mask                      255.255.255.0
  Remote Network
    Starting IP Address              10.0.0.0
    Subnet Mask                      255.0.0.0

IKE Tunnel Setting (IKE Phase 1)
  Authentication For Activating VPN
    Authenticated By
      User Name
      Password
  Negotiation Mode                   Main Mode
  Encryption Algorithm               DES
  Authentication Algorithm           MD5
  Key Group                          DH1
  SA Life Time                       28800 (Seconds)
  Pre-Shared Key                     12345678

IPSec Setting (IKE Phase 2)
  Encapsulation Mode                 Tunnel Mode
  IPSec Protocol                     ESP
  Encryption Algorithm               DES
  Authentication Algorithm           SHA1
  SA Life Time                       28800 (Seconds)
  Perfect Forward Secrecy (PFS)      None
```

The following table describes the labels in this screen.

**Table 19** VPN Wizard: VPN Status

| LABEL | DESCRIPTION |
|---|---|
| Gateway Policy Property | |
| Name | This is the name of this VPN gateway policy. |
| Gateway Policy Setting | |
| My ZyWALL | This is the WAN IP address or the domain name of your ZyWALL in router mode or the ZyWALL's IP address in bridge mode. |
| Remote Gateway Address | This is the IP address or the domain name used to identify the remote IPSec router. |
| Network Policy Property | |
| Active | This displays whether this VPN network policy is enabled or not. |
| Name | This is the name of this VPN network policy. |
| Network Policy Setting | |
| Local Network | |
| Starting IP Address | This is a (static) IP address on the LAN behind your ZyWALL. |
| Ending IP Address/ Subnet Mask | When the local network is configured for a single IP address, this field is N/A. When the local network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the local network is configured for a subnet, this is a subnet mask on the LAN behind your ZyWALL. |
| Remote Network | |
| Starting IP Address | This is a (static) IP address on the network behind the remote IPSec router. |
| Ending IP Address/ Subnet Mask | When the remote network is configured for a single IP address, this field is N/A. When the remote network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote network is configured for a subnet, this is a subnet mask on the network behind the remote IPSec router. |
| IKE Tunnel Setting (IKE Phase 1) | |
| Negotiation Mode | This shows **Main Mode** or **Aggressive Mode**. Multiple SAs connecting through a secure gateway must have the same negotiation mode. |
| Encryption Algorithm | This is the method of data encryption. Options can be **DES**, **3DES** or **AES**. |
| Authentication Algorithm | **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. |
| Key Group | This is the key group you chose for phase 1 IKE setup. |
| SA Life Time (Seconds) | This is the length of time before an IKE SA automatically renegotiates. |
| Pre-Shared Key | This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation. |
| IPSec Setting (IKE Phase 2) | |
| Encapsulation Mode | This shows **Tunnel** mode or **Transport** mode. |

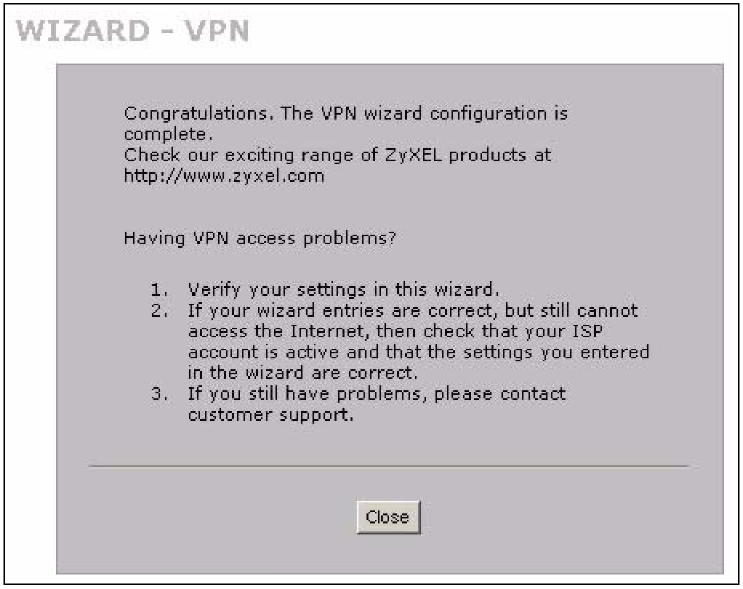
**Table 19** VPN Wizard: VPN Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| IPSec Protocol | **ESP** or **AH** are the security protocols used for an SA. |
| Encryption Algorithm | This is the method of data encryption. Options can be **DES**, **3DES**, **AES** or **NULL**. |
| Authentication Algorithm | **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. |
| SA Life Time (Seconds) | This is the length of time before an IKE SA automatically renegotiates. |
| Perfect Forward Secret (PFS) | Perfect Forward Secret (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. Otherwise, **DH1** or **DH2** are selected to enable PFS. |
| Back | Click **Back** to return to the previous screen. |
| Finish | Click **Finish** to complete and save the wizard setup. |

## 3.8 VPN Wizard Setup Complete

Congratulations! You have successfully set up the VPN rule for your ZyWALL. If you already had VPN rules configured, the wizard adds the new VPN rule after the last existing VPN rule.

**Figure 31** VPN Wizard Setup Complete



Congratulations. The VPN wizard configuration is complete.
Check our exciting range of ZyXEL products at http://www.zyxel.com

Having VPN access problems?

1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.

# 4

# Tutorials

This chapter describes

- how to apply security settings to VPN traffic.
- how to set up your ZyWALL if you have more than one fixed (static) IP address from your ISP.
- how to allocate bandwidth and apply priorities to traffic that flows out through the ZyWALL's WAN port.

## 4.1 Security Settings for VPN Traffic

The ZyWALL can apply the firewall and content filtering to the traffic going to or from the ZyWALL's VPN tunnels. The ZyWALL applies the security settings to the traffic before encrypting VPN traffic that it sends out or after decrypting received VPN traffic.

The security settings apply to VPN traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).

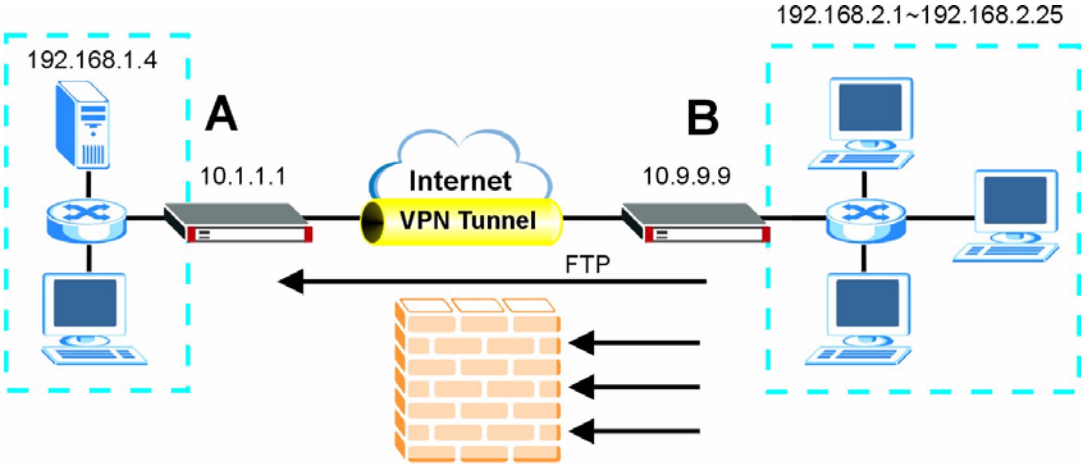
You can turn on content filtering for all of the ZyWALL's VPN traffic (regardless of its direction of travel). You can apply firewall security to VPN traffic based on its direction of travel. The following examples show how you do this for the firewall.

### 4.1.1 Firewall Rule for VPN Example

The firewall provides even more fine-tuned control for VPN tunnels. You can configure default and custom firewall rules for VPN packets.

Take the following example. You have a LAN FTP server with IP address 192.168.1.4 behind device A. You could configure a VPN rule to allow the network behind device B to access your LAN FTP server through a VPN tunnel. Now, if you don't want other services like chat or e-mail going to the FTP server, you can configure firewall rules that allow only FTP traffic to come from VPN tunnels to the FTP server. Furthermore, you can configure the firewall rule so that only the network behind device B can access the FTP server through a VPN tunnel (not other remote networks that have VPN tunnels with the ZyWALL).

**Figure 32** Firewall Rule for VPN

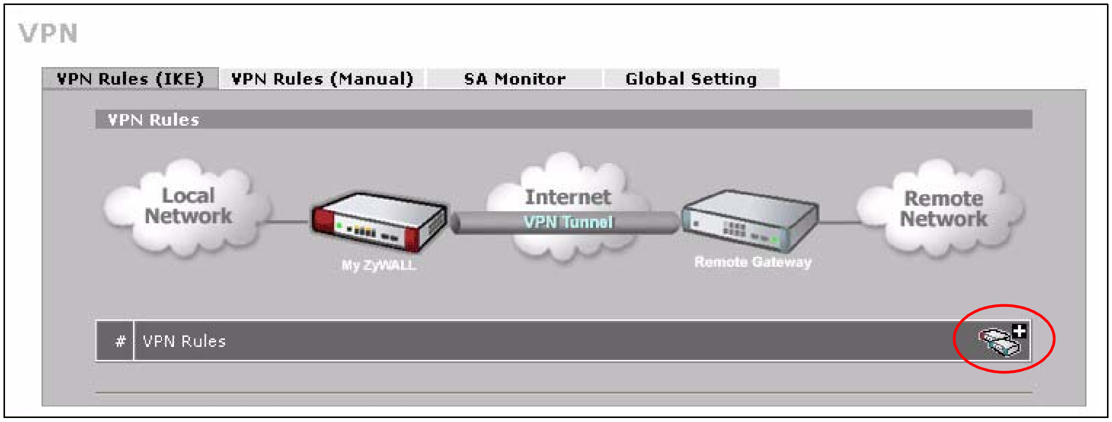

192.168.2.1~192.168.2.25
192.168.1.4
A
B
10.1.1.1
Internet
10.9.9.9
VPN Tunnel
FTP

## 4.1.2 Configuring the VPN Rule

This section shows how to configure a VPN rule on device **A** to let the network behind **B** access the FTP server. You would also have to configure a corresponding rule on device **B**.

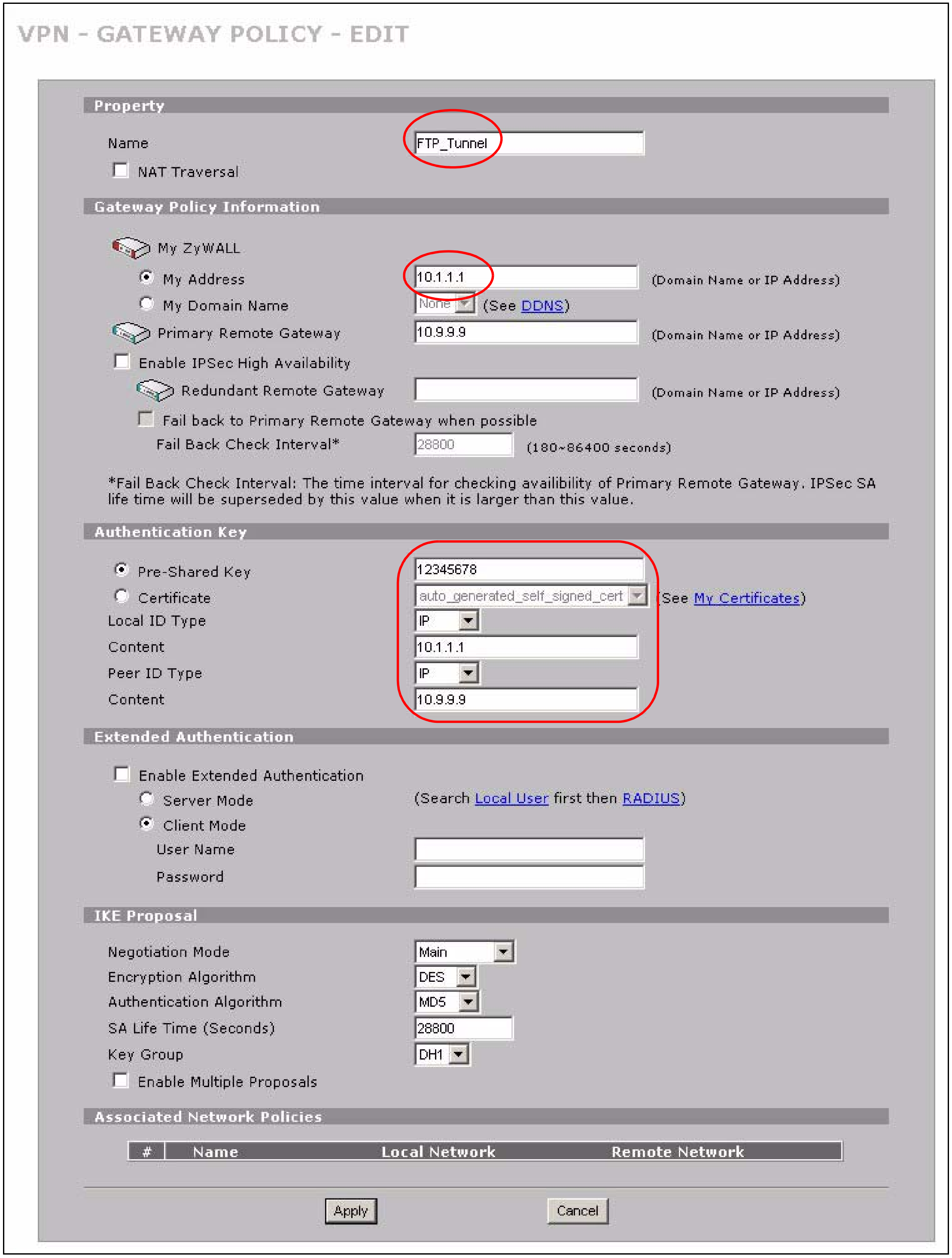
1 Click **Security** > **VPN** to open the following screen. Click the **Add Gateway Policy** icon.

**Figure 33** SECURITY > VPN > VPN Rules (IKE)


VPN
VPN Rules (IKE)
VPN Rules (Manual)
SA Monitor
Global Setting
VPN Rules
Local Network
Internet
VPN Tunnel
Remote Network
My ZyWALL
Remote Gateway
#
VPN Rules

2 Use this screen to set up the connection between the routers. Configure the fields that are circled as follows and click **Apply**.

**Figure 34** SECURITY > VPN > VPN Rules (IKE)> Add Gateway Policy



VPN - GATEWAY POLICY - EDIT

**Property**

Name: FTP_Tunnel

☐ NAT Traversal

**Gateway Policy Information**

My ZyWALL

● My Address: 10.1.1.1 (Domain Name or IP Address)

○ My Domain Name: None (See DDNS)

Primary Remote Gateway: 10.9.9.9 (Domain Name or IP Address)

☐ Enable IPSec High Availability

Redundant Remote Gateway: (Domain Name or IP Address)

☐ Fail back to Primary Remote Gateway when possible

Fail Back Check Interval*: 28800 (180~86400 seconds)

*Fail Back Check Interval: The time interval for checking availibility of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.

**Authentication Key**

● Pre-Shared Key: 12345678

○ Certificate: auto_generated_self_signed_cert (See My Certificates)

Local ID Type: IP

Content: 10.1.1.1

Peer ID Type: IP

Content: 10.9.9.9

**Extended Authentication**

☐ Enable Extended Authentication

○ Server Mode (Search Local User first then RADIUS)

● Client Mode

User Name:

Password:

**IKE Proposal**

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

SA Life Time (Seconds): 28800

Key Group: DH1

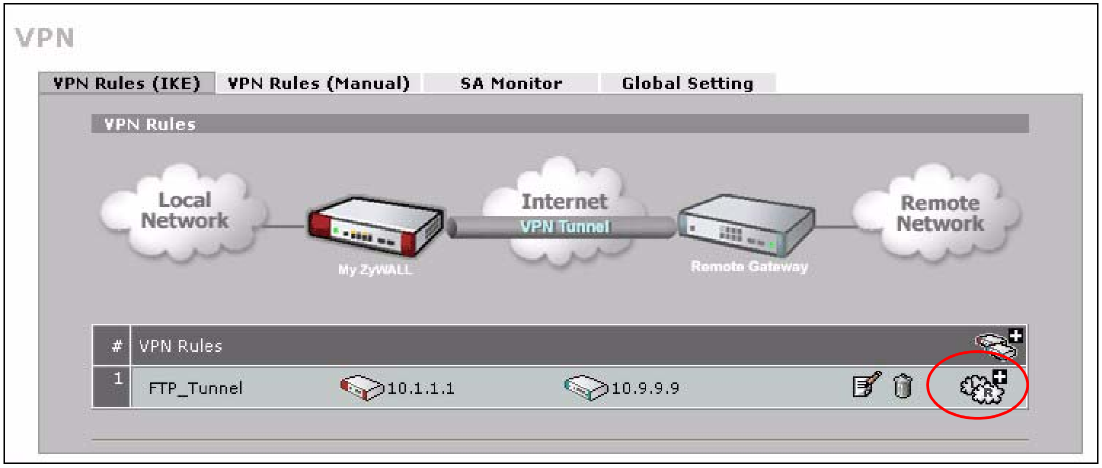
☐ Enable Multiple Proposals

**Associated Network Policies**

| # | Name | Local Network | Remote Network |
|---|---|---|---|

3 Click the **Add Network Policy** icon.

**Figure 35** SECURITY > VPN > VPN Rules (IKE): With Gateway Policy Example

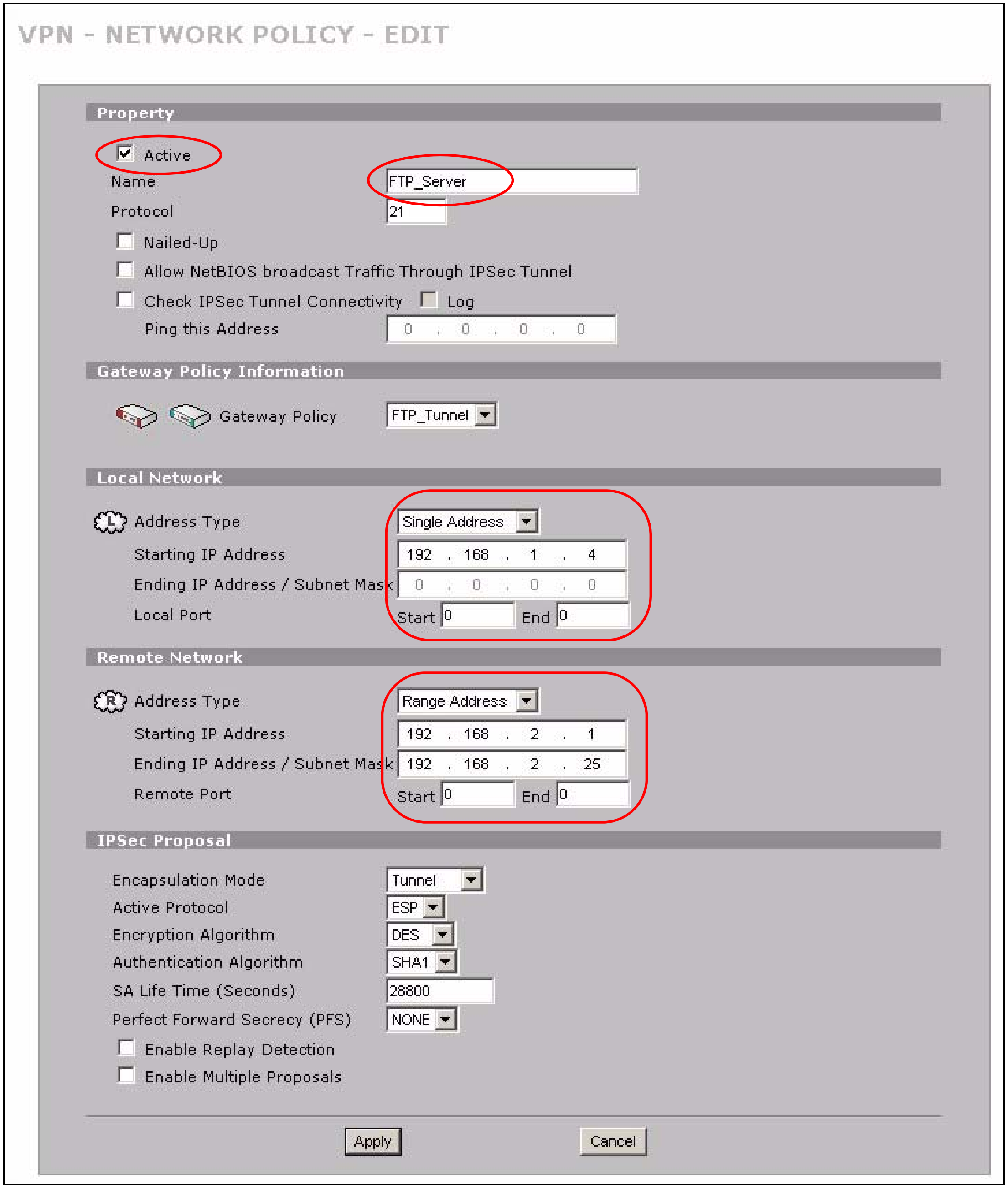

VPN
VPN Rules (IKE)
VPN Rules (Manual)
SA Monitor
Global Setting
VPN Rules
Local Network
Internet
VPN Tunnel
Remote Network
My ZyWALL
Remote Gateway

| # | VPN Rules | | |
|---|---|---|---|
| 1 | FTP_Tunnel | 10.1.1.1 | 10.9.9.9 |

4 Use this screen to specify which computers behind the routers can use the VPN tunnel. Configure the fields that are circled as follows and click **Apply**. You may notice that the example does not specify the port numbers. This is due to the following reasons.

- While FTP uses a control session on port 20, the port for the data session is not fixed. So this example uses the firewall's FTP application layer gateway (ALG) to handle this instead of specifying port numbers in this VPN network policy.
- The firewall provides better security because it operates at layer 4 and checks traffic sessions. The VPN network policy only operates at layer 3 and just checks IP addresses and port numbers.

**Figure 36** SECURITY > VPN > VPN Rules (IKE)> Add Network Policy



VPN - NETWORK POLICY - EDIT

Property

☑ Active
Name: FTP_Server
Protocol: 21
☐ Nailed-Up
☐ Allow NetBIOS broadcast Traffic Through IPSec Tunnel
☐ Check IPSec Tunnel Connectivity ☐ Log
Ping this Address: 0 . 0 . 0 . 0

Gateway Policy Information

Gateway Policy: FTP_Tunnel

Local Network

Address Type: Single Address
Starting IP Address: 192 . 168 . 1 . 4
Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0
Local Port: Start 0 End 0

Remote Network

Address Type: Range Address
Starting IP Address: 192 . 168 . 2 . 1
Ending IP Address / Subnet Mask: 192 . 168 . 2 . 25
Remote Port: Start 0 End 0

IPSec Proposal

Encapsulation Mode: Tunnel
Active Protocol: ESP
Encryption Algorithm: DES
Authentication Algorithm: SHA1
SA Life Time (Seconds): 28800
Perfect Forward Secrecy (PFS): NONE
☐ Enable Replay Detection
☐ Enable Multiple Proposals

## 4.1.3 Configuring the Firewall Rules

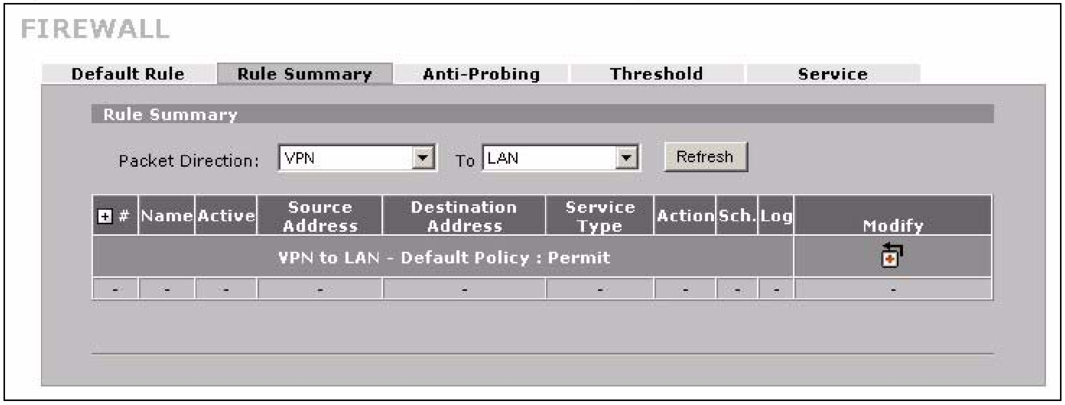
Suppose you have several VPN tunnels but you only want to allow device **B**’s network to access the FTP server. You also only want FTP traffic to go to the FTP server, so you want to block all other traffic types (like chat, e-mail, web and so on). The following sections show how to configure firewall rules to enforce these restrictions.

### 4.1.3.1 Firewall Rule to Allow Access Example

Configure a firewall rule that allows FTP access from the VPN tunnel to the FTP server.

1 Click **Security** > **Firewall** > **Rule Summary**.
2 Select **VPN** to **LAN** as the packet direction and click **Refresh**.
3 Click the insert icon.

**Figure 37** SECURITY > FIREWALL > Rule Summary

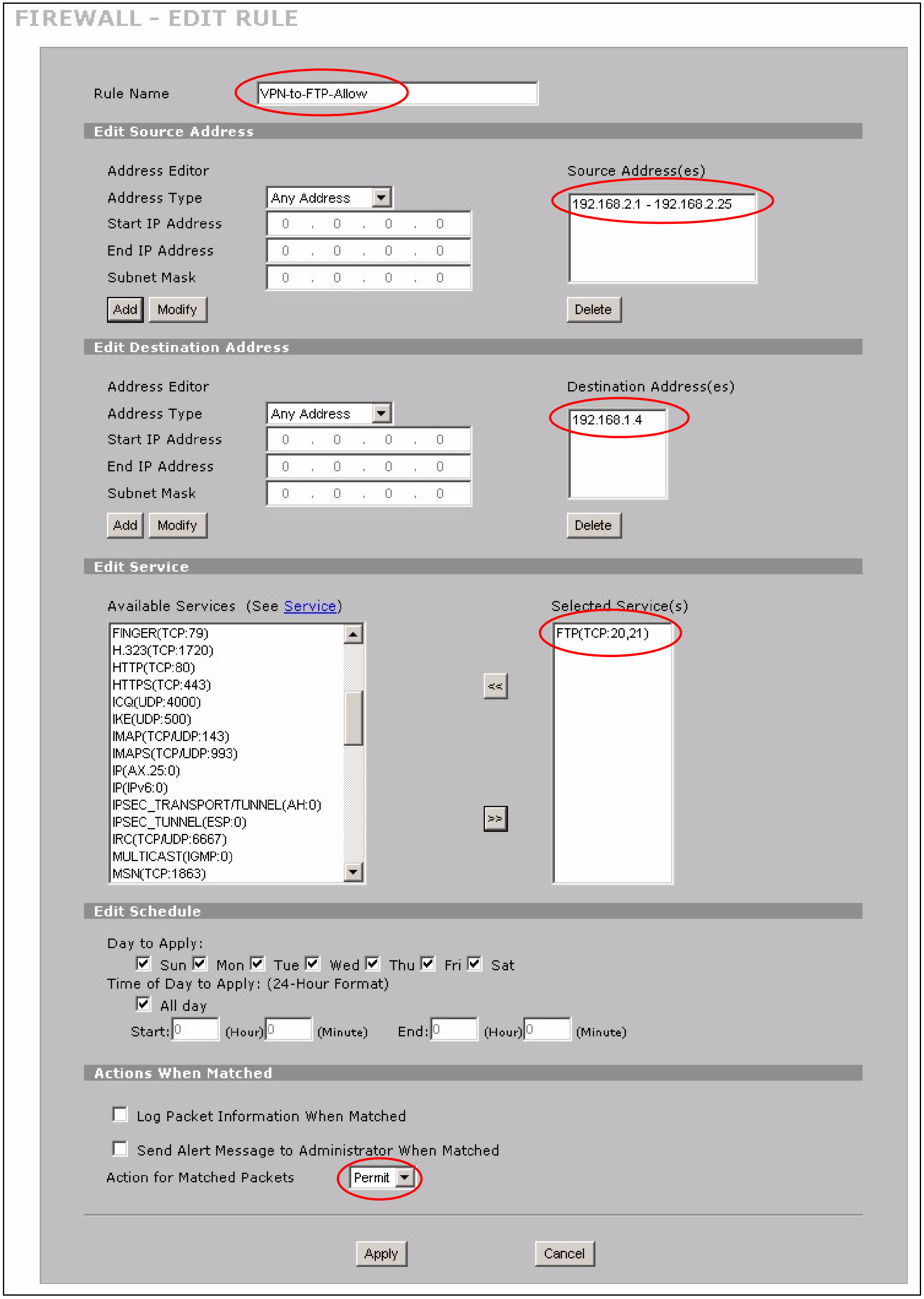

FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Rule Summary
Refresh

Packet Direction: VPN To LAN

| ⊞ # | Name | Active | Source Address | Destination Address | Service Type | Action | Sch. | Log | Modify |
|---|---|---|---|---|---|---|---|---|---|
| VPN to LAN - Default Policy : Permit | | | | | | | | | ⊞ |
| - | - | - | - | - | - | - | - | - | - |

4 Configure the rule as follows and click **Apply**. The source addresses are the VPN rule's remote network and the destination address is the LAN FTP server.

**Figure 38** SECURITY > FIREWALL > Rule Summary > Edit: Allow



FIREWALL - EDIT RULE

Rule Name: VPN-to-FTP-Allow

**Edit Source Address**

Address Editor

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Source Address(es): 192.168.2.1 - 192.168.2.25

**Edit Destination Address**

Address Editor

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Destination Address(es): 192.168.1.4

**Edit Service**

Available Services (See Service)

FINGER(TCP:79)
H.323(TCP:1720)
HTTP(TCP:80)
HTTPS(TCP:443)
ICQ(UDP:4000)
IKE(UDP:500)
IMAP(TCP/UDP:143)
IMAPS(TCP/UDP:993)
IP(AX.25:0)
IP(IPv6:0)
IPSEC_TRANSPORT/TUNNEL(AH:0)
IPSEC_TUNNEL(ESP:0)
IRC(TCP/UDP:6667)
MULTICAST(IGMP:0)
MSN(TCP:1863)

Selected Service(s): FTP(TCP:20,21)

**Edit Schedule**

Day to Apply:
☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Apply: (24-Hour Format)
☑ All day
Start: 0 (Hour) 0 (Minute) End: 0 (Hour) 0 (Minute)

**Actions When Matched**

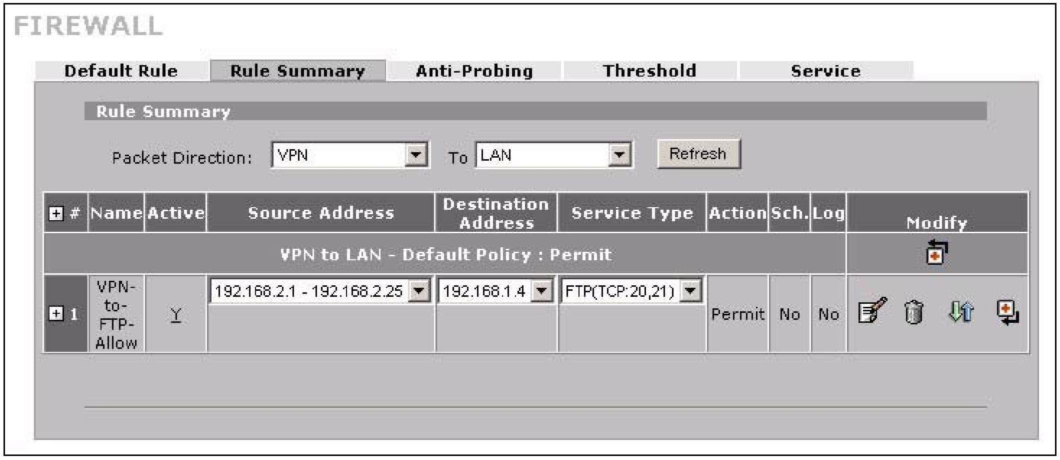
☐ Log Packet Information When Matched

☐ Send Alert Message to Administrator When Matched

Action for Matched Packets: Permit

**5** The rule displays in the summary list of VPN to LAN firewall rules.

**Figure 39** SECURITY > FIREWALL > Rule Summary: Allow


FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Rule Summary
Refresh

Packet Direction: VPN To LAN

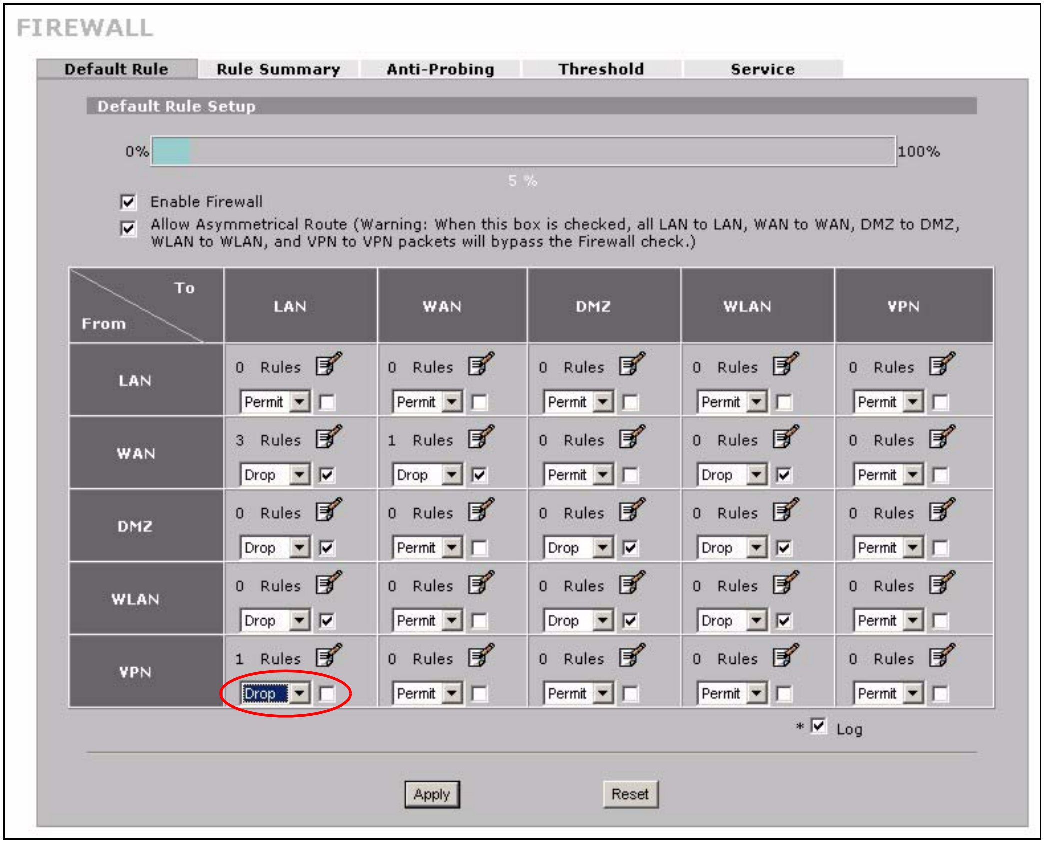
| # | Name | Active | Source Address | Destination Address | Service Type | Action | Sch. | Log | Modify |
|---|---|---|---|---|---|---|---|---|---|
| VPN to LAN - Default Policy : Permit | | | | | | | | | |
| 1 | VPN-to-FTP-Allow | Y | 192.168.2.1 - 192.168.2.25 | 192.168.1.4 | FTP(TCP:20,21) | Permit | No | No | |

## 4.1.3.2 Default Firewall Rule to Block Other Access Example

Now you configure the default firewall rule to block all VPN to LAN traffic. This blocks any other types of access from VPN tunnels to the LAN FTP server. This means that you need to configure more firewall rules if you want to allow any other VPN tunnels to access the LAN.

1. Click **SECURITY** > **FIREWALL** > **Default Rule**.
2. Configure the screen as follows and click **Apply**.

**Figure 40** SECURITY > FIREWALL > Default Rule: Block From VPN To LAN


FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Default Rule Setup
0%
100%
5 %
Apply
Reset

☑ Enable Firewall

☑ Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ, WLAN to WLAN, and VPN to VPN packets will bypass the Firewall check.)

| From \ To | LAN | WAN | DMZ | WLAN | VPN |
|---|---|---|---|---|---|
| LAN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |
| WAN | 3 Rules<br>Drop ☑ | 1 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| DMZ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| WLAN | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| VPN | 1 Rules<br>Drop ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |

* ☑ Log

## 4.2 Using NAT with Multiple Public IP Addresses

This section shows you examples of how to set up your ZyWALL if you have more than one fixed (static) IP address from your ISP.

### 4.2.1 Example Parameters and Scenario

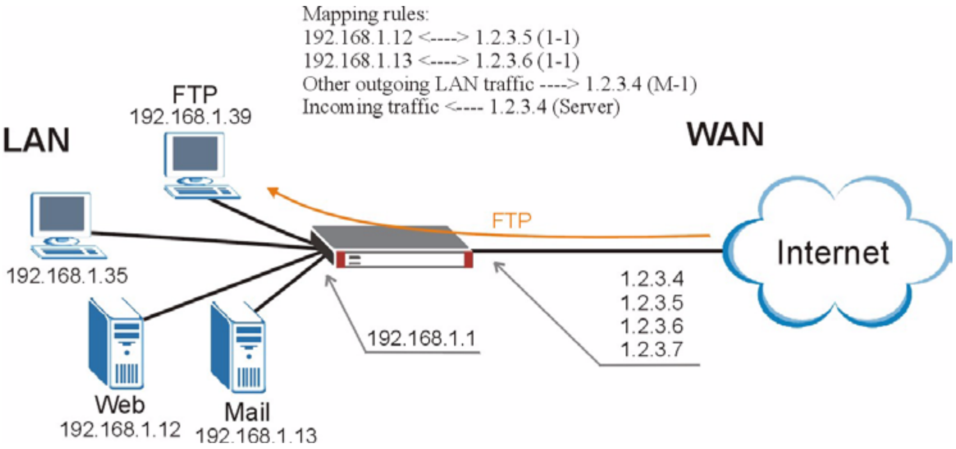
The following table shows the public IP addresses from your ISP and your ZyWALL's LAN IP address.

| | |
|---|---|
| **Public IP Addresses** | 1.2.3.4 to 1.2.3.7 |
| **ZyWALL's LAN IP Address** | 192.168.1.1 |

The following figure shows the network you want to set up in this example.

- Assign the first public address (1.2.3.4) to the ZyWALL's WAN port.
- Map the second and third public IP addresses (1.2.3.5 and 1.2.3.6) to the web and mail servers (192.168.1.12 and 192.168.1.13) respectively for traffic in both directions.
- Map the first public address (1.2.3.4) to outgoing traffic from other local computers.
- Map the first public address (1.2.3.4) to incoming traffic from the WAN.
- Forward FTP traffic using port 21 from the WAN to a specific local computer (192.168.1.39).
- The last public IP address (1.2.3.7) is not mapped to any device and is reserved for future use.

**Figure 41** Tutorial Example: Using NAT with Static Public IP Addresses


Mapping rules:
192.168.1.12 <----> 1.2.3.5 (1-1)
192.168.1.13 <----> 1.2.3.6 (1-1)
Other outgoing LAN traffic ----> 1.2.3.4 (M-1)
Incoming traffic <---- 1.2.3.4 (Server)
FTP
192.168.1.39
LAN
WAN
FTP
Internet
192.168.1.35
1.2.3.4
1.2.3.5
1.2.3.6
1.2.3.7
192.168.1.1
Web
192.168.1.12
Mail
192.168.1.13

To set up this network, we are going to:

1. Configure the WAN connection to use the first public IP address (1.2.3.4).
2. Configure NAT address mapping for other public IP addresses (1.2.3.5 and 1.2.3.6).
3. Configure NAT port forwarding to forward FTP traffic from the WAN to a specific computer on your local network.

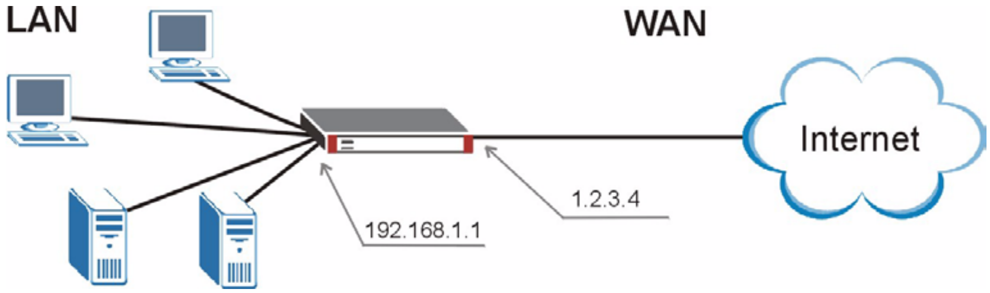
## 4.2.2 Configuring the WAN Connection with a Static IP Address

The following table shows the information your ISP gave you for Internet connection.

| | |
|---|---|
| **Encapsulation** | PPPoE |
| **Public IP Addresses** | 1.2.3.4<br>1.2.3.5<br>1.2.3.6<br>1.2.3.7 |
| **Gateway IP Address** | 1.2.3.89 |
| **Subnet Mask** | 255.255.255.0 |
| **User Name** | exampleuser |
| **Password** | abcd1234 |
| **DNS Server** | 1.2.1.1<br>1.2.1.2 |

Follow the steps below to configure your ZyWALL for Internet access using PPPoE in this example.

**Figure 42** Tutorial Example: WAN Connection with a Static Public IP Address



1 Click **NETWORK** > **WAN** > **WAN**.

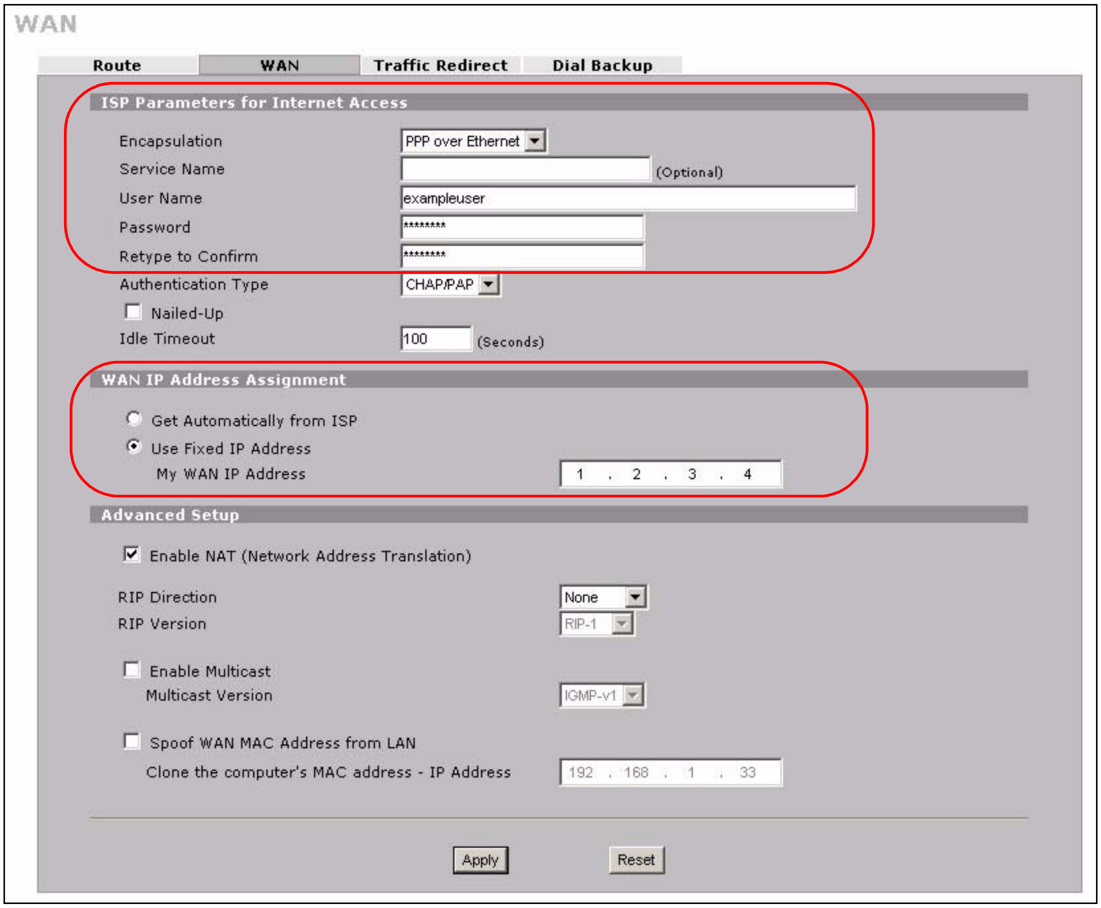
2 Select **PPPoE** (**PPP over Ethernet**) from the **Encapsulation** drop-down list box.

3 In the **ISP Parameters for Internet Access** section, enter the information (such as the user name and password) provided by your ISP. If your ISP didn’t give you the service name, leave the field blank.

4 In the **WAN IP Address Assignment** section, select **Use Fixed IP Address** and enter the first fixed public IP address (1.2.3.4 in this example).

5 Click **Apply**.

**Figure 43** Tutorial Example: WAN Screen



ISP Parameters for Internet Access

Encapsulation: PPP over Ethernet
Service Name: (Optional)
User Name: exampleuser
Password: ********
Retype to Confirm: ********
Authentication Type: CHAP/PAP
☐ Nailed-Up
Idle Timeout: 100 (Seconds)

WAN IP Address Assignment

○ Get Automatically from ISP
● Use Fixed IP Address
My WAN IP Address: 1 . 2 . 3 . 4

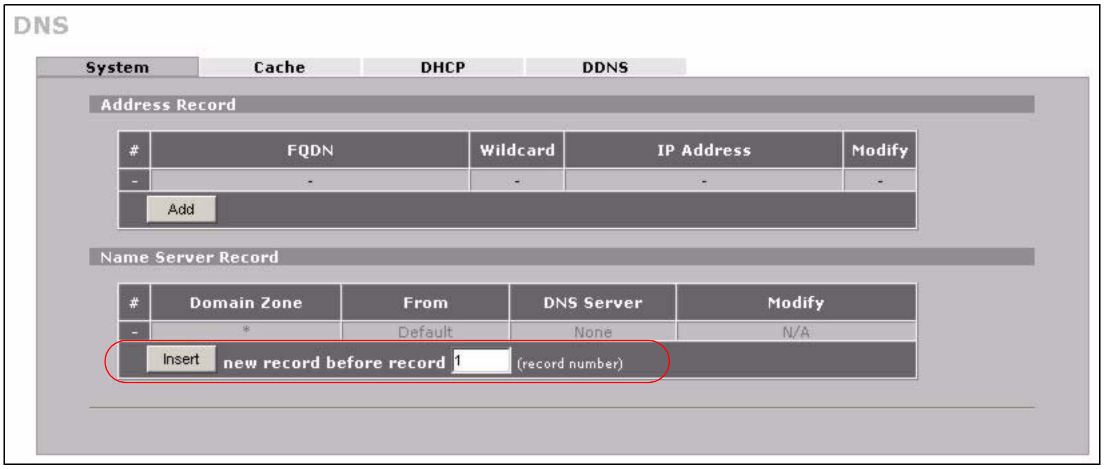
Advanced Setup

☑ Enable NAT (Network Address Translation)
RIP Direction: None
RIP Version: RIP-1
☐ Enable Multicast
Multicast Version: IGMP-v1
☐ Spoof WAN MAC Address from LAN
Clone the computer's MAC address - IP Address: 192 . 168 . 1 . 33

6 Click **ADVANCED** > **DNS**.

7 The **System** screen displays. Click the **Insert** button to configure the IP address of the DNS server the ZyWALL can query to resolve domain names.

**Figure 44** Tutorial Example: DNS > System



Address Record

| # | FQDN | Wildcard | IP Address | Modify |
|---|---|---|---|---|
| - | - | - | - | - |

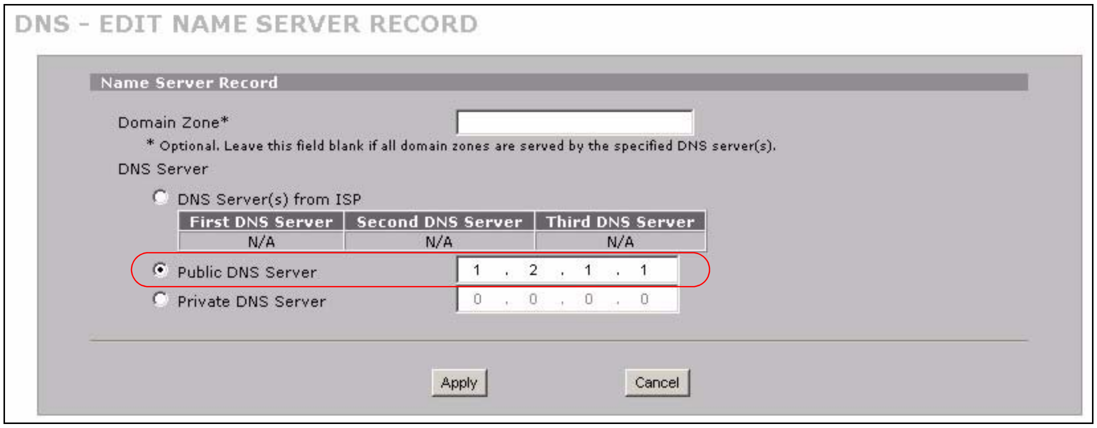
Name Server Record

| # | Domain Zone | From | DNS Server | Modify |
|---|---|---|---|---|
| - | * | Default | None | N/A |

Insert new record before record 1 (record number)

8 Select **Public DNS Server** and enter the first DNS server's IP address given by your ISP. Click **Apply**.

**Figure 45** Tutorial Example: DNS > System Edit-1



DNS - EDIT NAME SERVER RECORD

Name Server Record

Domain Zone*

* Optional. Leave this field blank if all domain zones are served by the specified DNS server(s).

DNS Server

○ DNS Server(s) from ISP

| First DNS Server | Second DNS Server | Third DNS Server |
|---|---|---|
| N/A | N/A | N/A |

● Public DNS Server 1 . 2 . 1 . 1

○ Private DNS Server 0 . 0 . 0 . 0

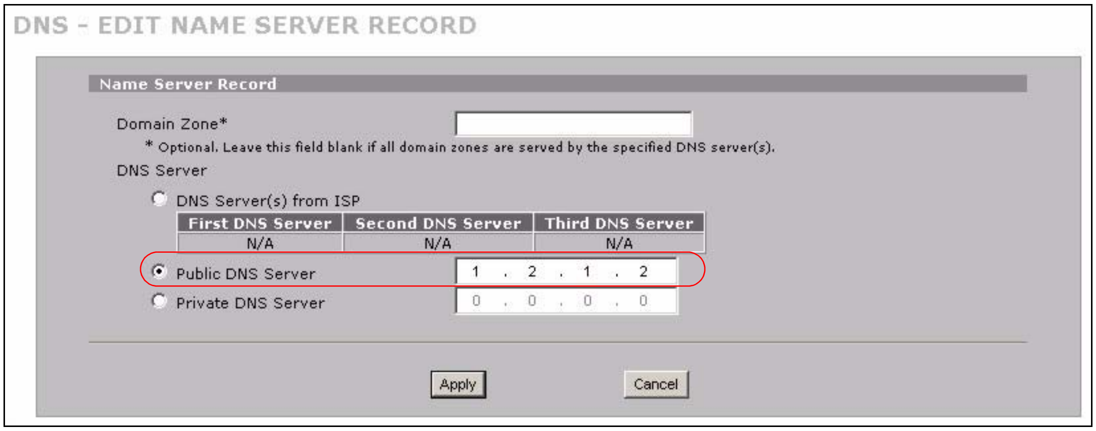
9 Enter the rule number (2) where you want to put the second record and click the **Insert** button to configure the second DNS server's IP address as follows. Click **Apply**.

---

To resolve a domain name, theZyWALL checks it against the name server record entries in the order that they appear in this list.

---

**Figure 46** Tutorial Example: DNS > System Edit-2



DNS - EDIT NAME SERVER RECORD

Name Server Record

Domain Zone*

* Optional. Leave this field blank if all domain zones are served by the specified DNS server(s).

DNS Server

○ DNS Server(s) from ISP

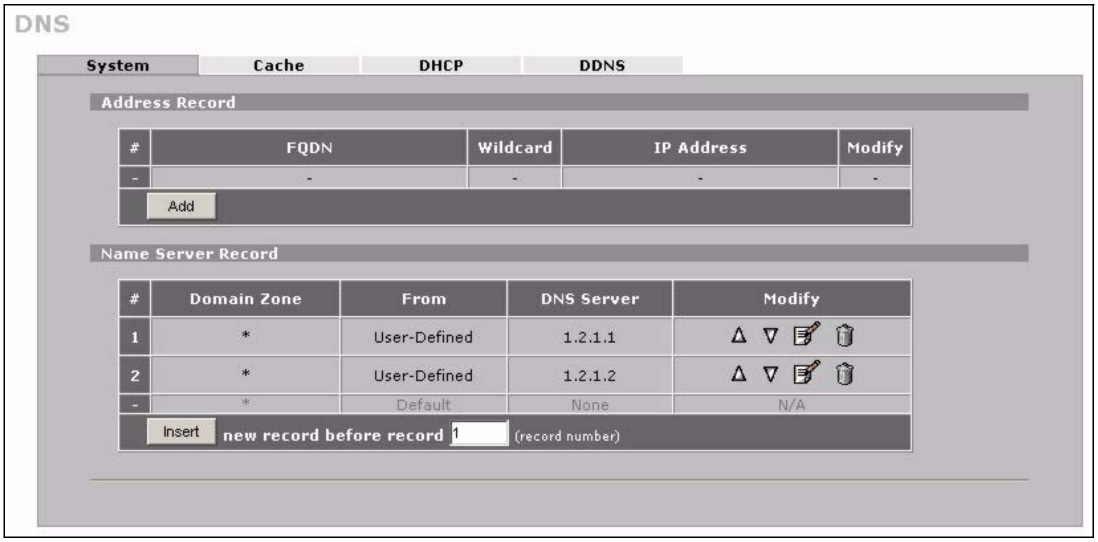
| First DNS Server | Second DNS Server | Third DNS Server |
|---|---|---|
| N/A | N/A | N/A |

● Public DNS Server 1 . 2 . 1 . 2

○ Private DNS Server 0 . 0 . 0 . 0

10 The **DNS** > **System** screen should look as shown.

**Figure 47** Tutorial Example: DNS > System: Done



Address Record

| # | FQDN | Wildcard | IP Address | Modify |
|---|---|---|---|---|
| - | - | - | - | - |

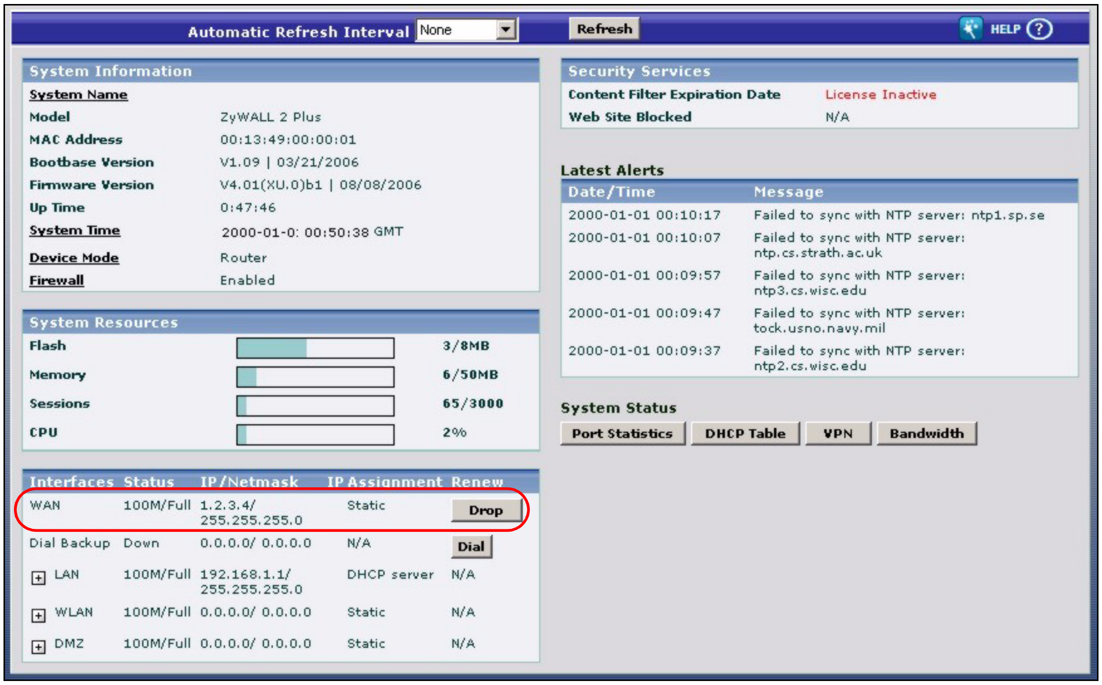
Name Server Record

| # | Domain Zone | From | DNS Server | Modify |
|---|---|---|---|---|
| 1 | * | User-Defined | 1.2.1.1 | Δ ∇ |
| 2 | * | User-Defined | 1.2.1.2 | Δ ∇ |
| - | * | Default | None | N/A |

Insert new record before record 1 (record number)

**11** Go to the **Home** screen to check your WAN connection status. Make sure the status is not down.

**Figure 48** Tutorial Example: Status



System Information

| | |
|---|---|
| System Name | |
| Model | ZyWALL 2 Plus |
| MAC Address | 00:13:49:00:00:01 |
| Bootbase Version | V1.09 \| 03/21/2006 |
| Firmware Version | V4.01(XU.0)b1 \| 08/08/2006 |
| Up Time | 0:47:46 |
| System Time | 2000-01-0: 00:50:38 GMT |
| Device Mode | Router |
| Firewall | Enabled |

System Resources

| | |
|---|---|
| Flash | 3/8MB |
| Memory | 6/50MB |
| Sessions | 65/3000 |
| CPU | 2% |

| Interfaces | Status | IP/Netmask | IP Assignment | Renew |
|---|---|---|---|---|
| WAN | 100M/Full | 1.2.3.4/ 255.255.255.0 | Static | Drop |
| Dial Backup | Down | 0.0.0.0/ 0.0.0.0 | N/A | Dial |
| + LAN | 100M/Full | 192.168.1.1/ 255.255.255.0 | DHCP server | N/A |
| + WLAN | 100M/Full | 0.0.0.0/ 0.0.0.0 | Static | N/A |
| + DMZ | 100M/Full | 0.0.0.0/ 0.0.0.0 | Static | N/A |

Security Services

| | |
|---|---|
| Content Filter Expiration Date | License Inactive |
| Web Site Blocked | N/A |

Latest Alerts

| Date/Time | Message |
|---|---|
| 2000-01-01 00:10:17 | Failed to sync with NTP server: ntp1.sp.se |
| 2000-01-01 00:10:07 | Failed to sync with NTP server: ntp.cs.strath.ac.uk |
| 2000-01-01 00:09:57 | Failed to sync with NTP server: ntp3.cs.wisc.edu |
| 2000-01-01 00:09:47 | Failed to sync with NTP server: tock.usno.navy.mil |
| 2000-01-01 00:09:37 | Failed to sync with NTP server: ntp2.cs.wisc.edu |

System Status

## 4.2.3 Public IP Address Mapping

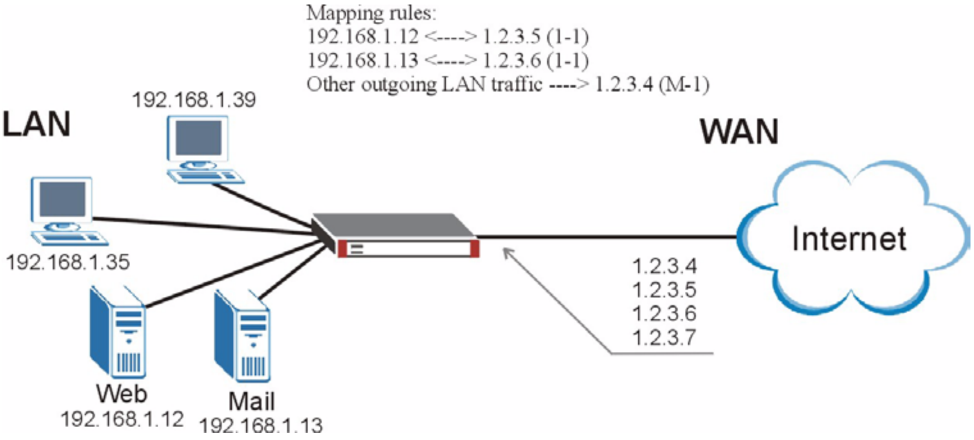
To have the local computers and servers use specific WAN IP addresses, you need to map static public IP addresses to them.

The one-to-one NAT address mapping rules are for both incoming and outgoing connections. The ZyWALL forwards traffic that is initiated from either the LAN or the WAN to the destination IP address.

The many-to-one or many-to-many NAT address mapping rules are for outgoing connections only. That means only traffic initiated from the LAN or returned packets are allowed to go through the ZyWALL.

In this example, you create two one-to-one rules to map the internal web server (192.168.1.12) and mail server (192.168.1.13) to different static public IP addresses. The many-to-one rule maps a public IP address (1.2.3.4, that is, the ZyWALL's WAN IP address) to outgoing LAN traffic. It allows other local computers on the same subnet as the ZyWALL's LAN IP address to use this IP address to access the Internet.

**Figure 49** Tutorial Example: Mapping Multiple Public IP Addresses to Inside Servers

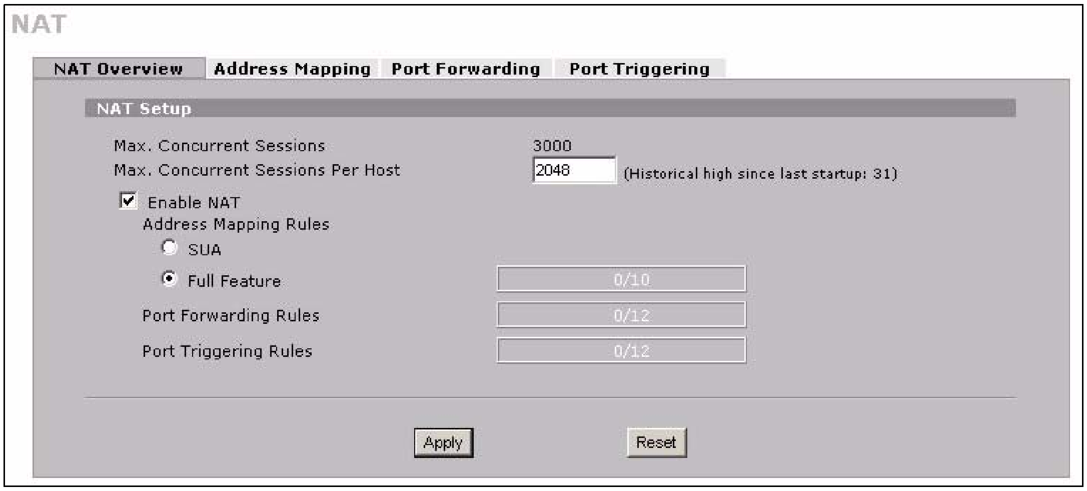

Mapping rules:
192.168.1.12 <----> 1.2.3.5 (1-1)
192.168.1.13 <----> 1.2.3.6 (1-1)
Other outgoing LAN traffic ----> 1.2.3.4 (M-1)
192.168.1.39
LAN
WAN
192.168.1.35
Internet
1.2.3.4
1.2.3.5
1.2.3.6
1.2.3.7
Web
192.168.1.12
Mail
192.168.1.13

The ZyWALL applies the rules in the order that you specify. You should put any one-to-one rules before a many-to-one rule.

1 Click **ADVANCED** > **NAT**.

2 Enable NAT and select **Full Feature** as you have multiple public IP addresses to map to private IP addresses. Click **Apply**.

**Figure 50** Tutorial Example: NAT > NAT Overview


NAT
NAT Overview
Address Mapping
Port Forwarding
Port Triggering
NAT Setup
Apply
Reset

Max. Concurrent Sessions 3000

Max. Concurrent Sessions Per Host 2048 (Historical high since last startup: 31)

☑ Enable NAT

Address Mapping Rules

○ SUA

● Full Feature 0/10

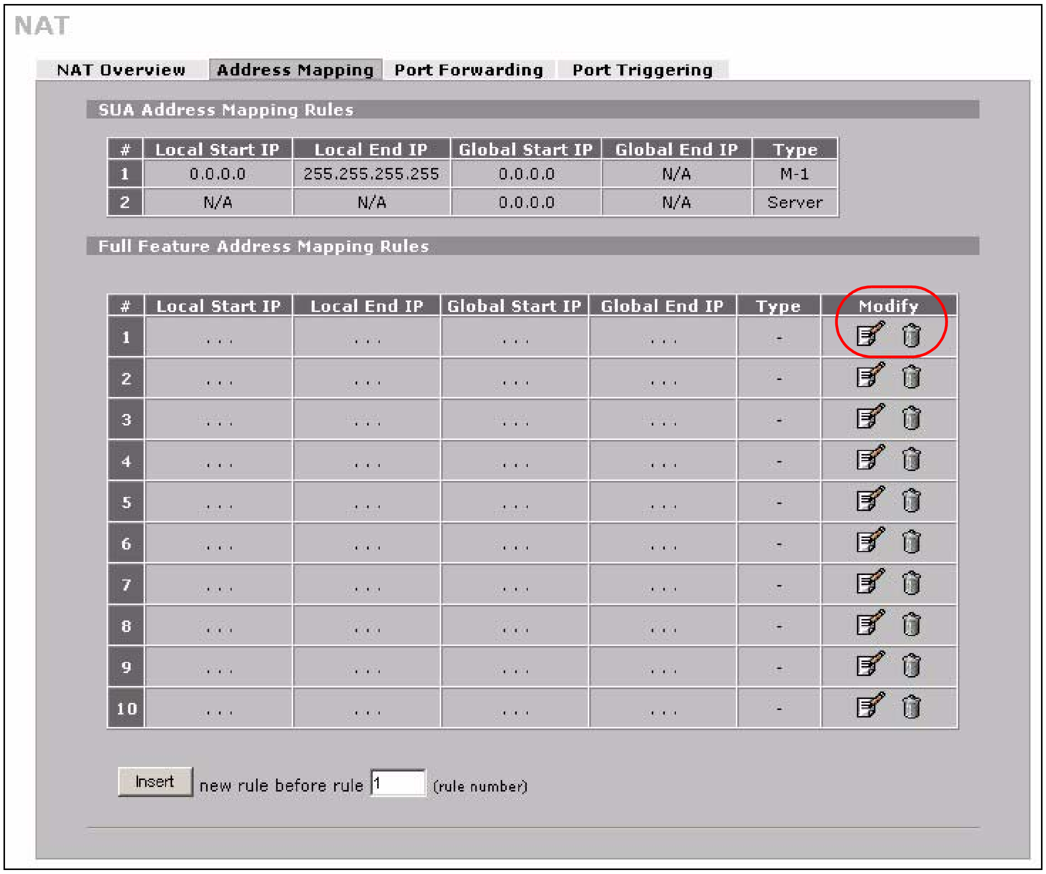
Port Forwarding Rules 0/12

Port Triggering Rules 0/12

3 Click the **Address Mapping** tab.

4 Click the first rule's **Edit** icon (📝) in the **Modify** column to display the **Address Mapping Rule** screen.

**Figure 51** Tutorial Example: NAT > Address Mapping


NAT
NAT Overview
Address Mapping
Port Forwarding
Port Triggering
Insert

SUA Address Mapping Rules

| # | Local Start IP | Local End IP | Global Start IP | Global End IP | Type |
|---|---|---|---|---|---|
| 1 | 0.0.0.0 | 255.255.255.255 | 0.0.0.0 | N/A | M-1 |
| 2 | N/A | N/A | 0.0.0.0 | N/A | Server |

Full Feature Address Mapping Rules

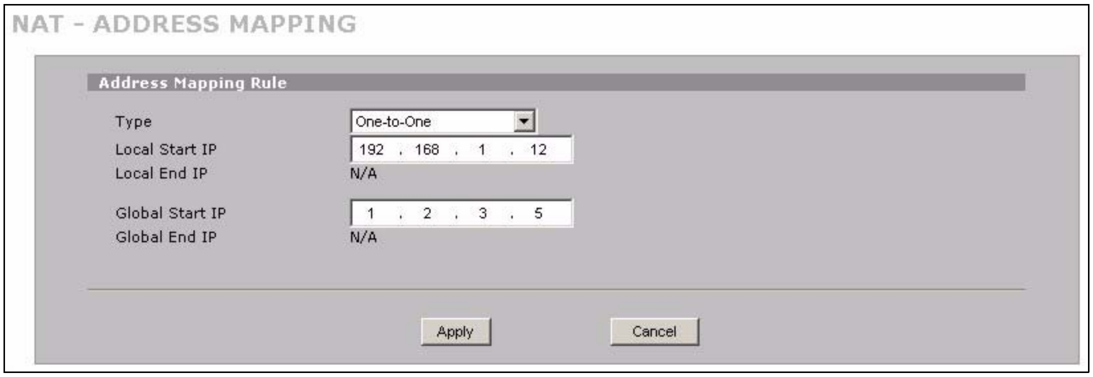
| # | Local Start IP | Local End IP | Global Start IP | Global End IP | Type | Modify |
|---|---|---|---|---|---|---|
| 1 | ... | ... | ... | ... | - | 📝 🗑 |
| 2 | ... | ... | ... | ... | - | 📝 🗑 |
| 3 | ... | ... | ... | ... | - | 📝 🗑 |
| 4 | ... | ... | ... | ... | - | 📝 🗑 |
| 5 | ... | ... | ... | ... | - | 📝 🗑 |
| 6 | ... | ... | ... | ... | - | 📝 🗑 |
| 7 | ... | ... | ... | ... | - | 📝 🗑 |
| 8 | ... | ... | ... | ... | - | 📝 🗑 |
| 9 | ... | ... | ... | ... | - | 📝 🗑 |
| 10 | ... | ... | ... | ... | - | 📝 🗑 |

Insert new rule before rule 1 (rule number)

5 Map a public IP address to the web server.

Select the **One-to-One** type and enter 192.168.1.12 as the local start IP address and 1.2.3.5 as the global start IP address. Click **Apply**.

**Figure 52** Tutorial Example: NAT Address Mapping Edit: One-to-One (1)



NAT - ADDRESS MAPPING

Address Mapping Rule

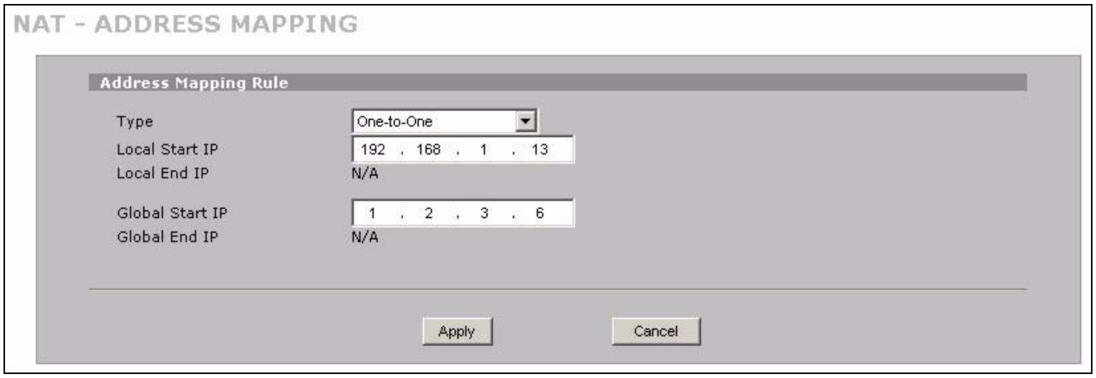
Type: One-to-One
Local Start IP: 192 . 168 . 1 . 12
Local End IP: N/A
Global Start IP: 1 . 2 . 3 . 5
Global End IP: N/A

**6** Click the second rule's **Edit** icon (✎).

**7** Map a public IP address to the mail server.

Select the **One-to-One** type and enter 192.168.1.13 as the local start IP address and 1.2.3.6 as the global start IP address. Click **Apply**.

**Figure 53** Tutorial Example: NAT Address Mapping Edit: One-to-One (2)



NAT - ADDRESS MAPPING

Address Mapping Rule

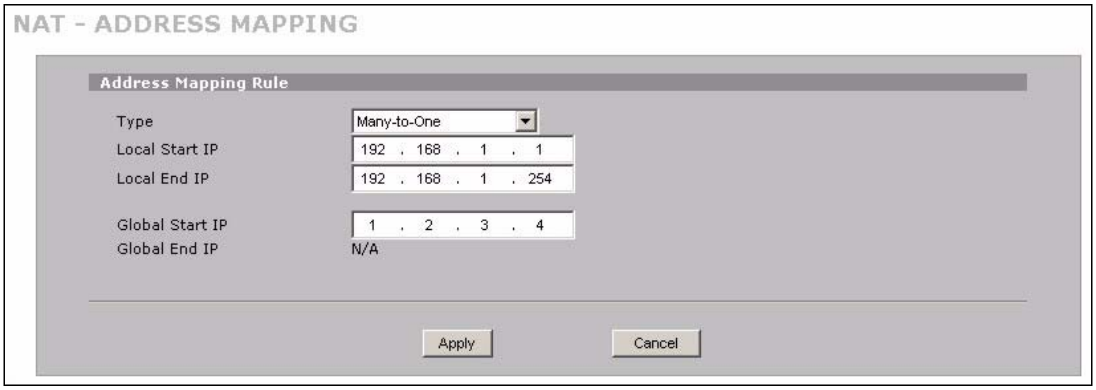
Type: One-to-One
Local Start IP: 192 . 168 . 1 . 13
Local End IP: N/A
Global Start IP: 1 . 2 . 3 . 6
Global End IP: N/A

**8** Click the third rule's **Edit** icon (✎).

**9** Map a public IP address to other outgoing LAN traffic.

Select the **Many-to-One** type and enter 192.168.1.1 as the local start IP address, 192.168.1.254 as the local end IP address and 1.2.3.4 as the global start IP address. Click **Apply**.

**Figure 54** Tutorial Example: NAT Address Mapping Edit: Many-to-One



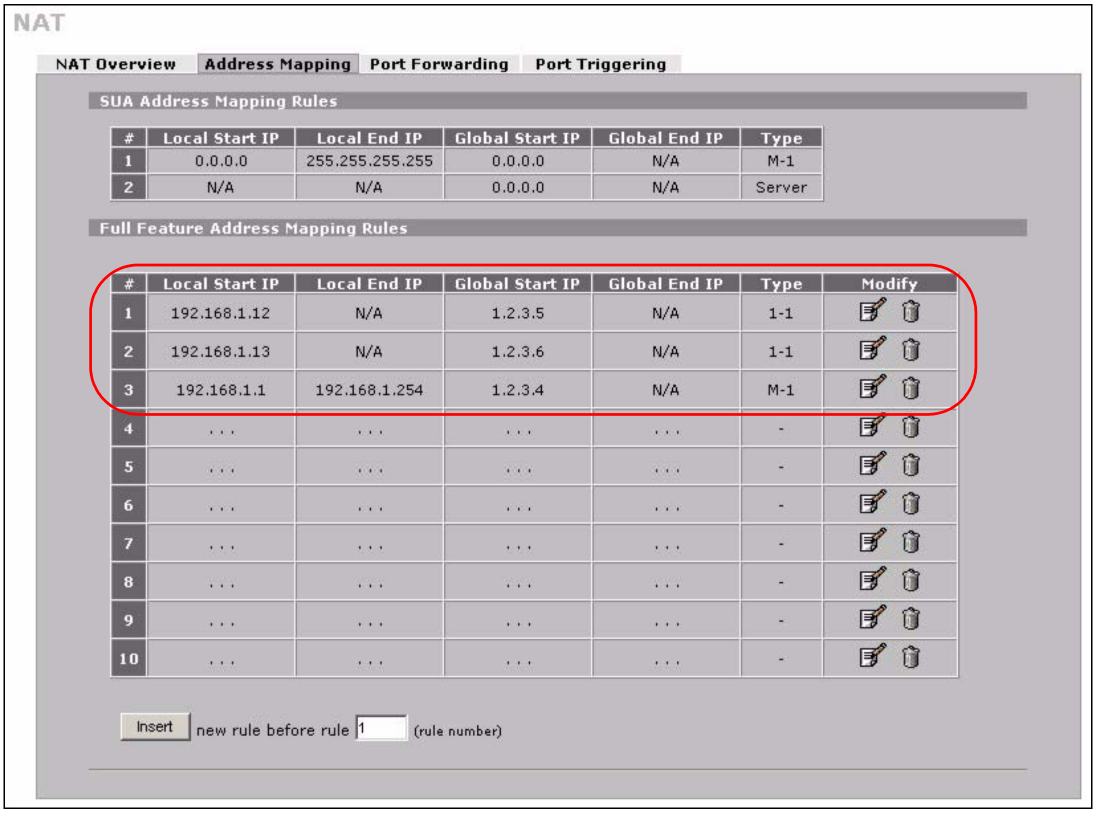
NAT - ADDRESS MAPPING

Address Mapping Rule

Type: Many-to-One
Local Start IP: 192 . 168 . 1 . 1
Local End IP: 192 . 168 . 1 . 254
Global Start IP: 1 . 2 . 3 . 4
Global End IP: N/A

**10** After the configurations, the **Address Mapping** screen looks as shown. You still have one IP address (1.2.3.7) that can be assigned to another internal server when you expand your network.

**Figure 55** Tutorial Example: NAT Address Mapping Done



SUA Address Mapping Rules

| # | Local Start IP | Local End IP | Global Start IP | Global End IP | Type |
|---|---|---|---|---|---|
| 1 | 0.0.0.0 | 255.255.255.255 | 0.0.0.0 | N/A | M-1 |
| 2 | N/A | N/A | 0.0.0.0 | N/A | Server |

Full Feature Address Mapping Rules

| # | Local Start IP | Local End IP | Global Start IP | Global End IP | Type | Modify |
|---|---|---|---|---|---|---|
| 1 | 192.168.1.12 | N/A | 1.2.3.5 | N/A | 1-1 | ✎ 🗑 |
| 2 | 192.168.1.13 | N/A | 1.2.3.6 | N/A | 1-1 | ✎ 🗑 |
| 3 | 192.168.1.1 | 192.168.1.254 | 1.2.3.4 | N/A | M-1 | ✎ 🗑 |
| 4 | ... | ... | ... | ... | - | ✎ 🗑 |
| 5 | ... | ... | ... | ... | - | ✎ 🗑 |
| 6 | ... | ... | ... | ... | - | ✎ 🗑 |
| 7 | ... | ... | ... | ... | - | ✎ 🗑 |
| 8 | ... | ... | ... | ... | - | ✎ 🗑 |
| 9 | ... | ... | ... | ... | - | ✎ 🗑 |
| 10 | ... | ... | ... | ... | - | ✎ 🗑 |

To allow traffic from the WAN to be forwarded through the ZyXEL Device, you must also create a firewall rule. Refer to Section 4.2.5 on page 107 for more information.

## 4.2.4 Forwarding Traffic from the WAN to a Local Computer

A server NAT address mapping rule allows computers behind the NAT be accessible to the outside world. To have the ZyWALL forward incoming traffic to a specific computer on your local network, you should also create a port forwarding (server mapping) rule.

In this example, you want to forward FTP traffic using port 21 to the computer with the IP address of 192.168.1.39.

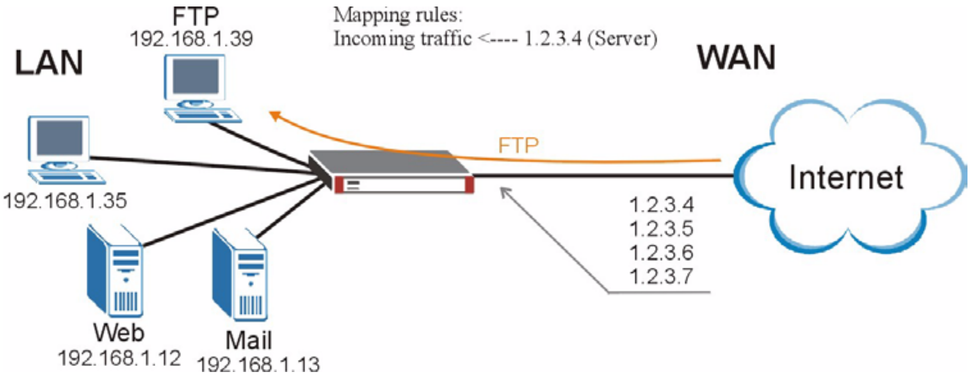
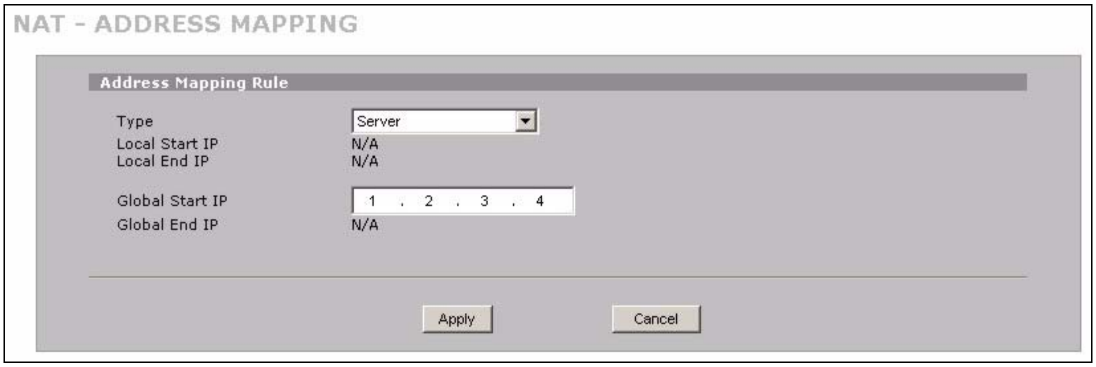

FTP
192.168.1.39
Mapping rules:
Incoming traffic <---- 1.2.3.4 (Server)
LAN
WAN
FTP
Internet
192.168.1.35
1.2.3.4
1.2.3.5
1.2.3.6
1.2.3.7
Web
192.168.1.12
Mail
192.168.1.13

**Figure 56** Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer

1 Click **ADVANCED** > **NAT** > **Address Mapping**.

2 Click the forth rule's **Edit** icon (📝) to configure a server rule.

**Figure 57** Tutorial Example: NAT Address Mapping Edit: Server

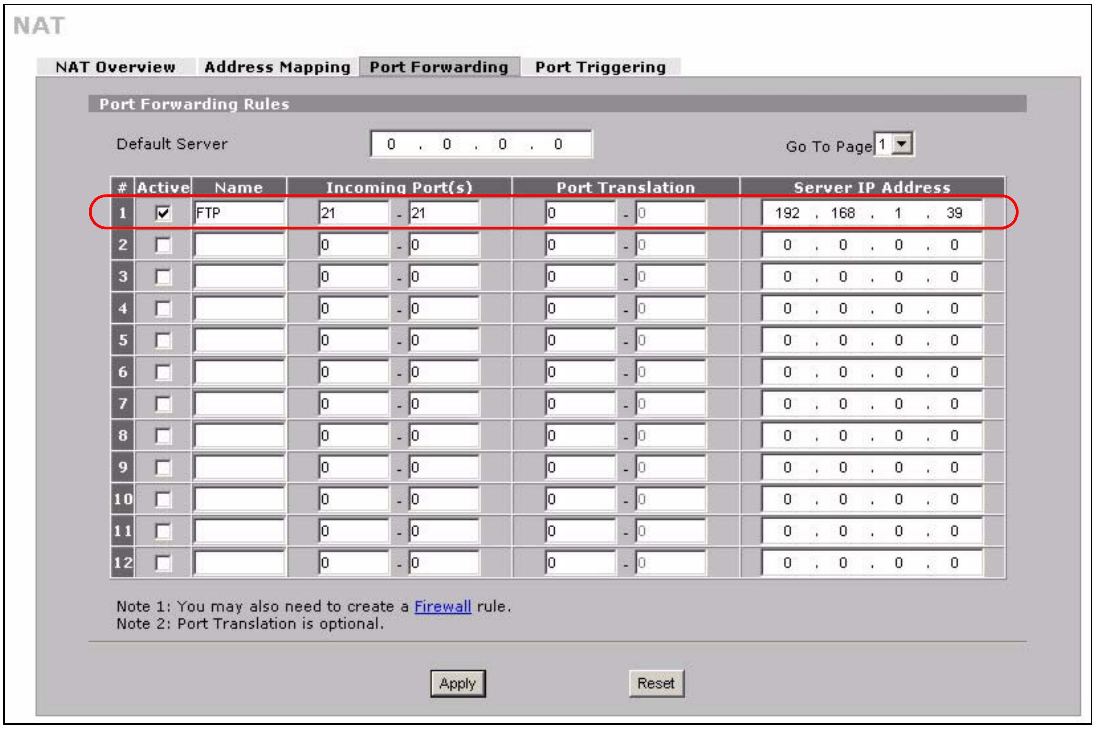

NAT - ADDRESS MAPPING
Address Mapping Rule
Apply
Cancel

| | |
|---|---|
| Type | Server |
| Local Start IP | N/A |
| Local End IP | N/A |
| Global Start IP | 1 . 2 . 3 . 4 |
| Global End IP | N/A |

3 Click the **Port Forwarding** tab.

4 Select the **Active** check box, enter a descriptive name (**FTP** for example), incoming port number (21) and 192.168.1.39 as the server IP address. Click **Apply**.

**Figure 58** Tutorial Example: NAT Port Forwarding



NAT
NAT Overview
Address Mapping
Port Forwarding
Port Triggering
Apply
Reset

Port Forwarding Rules

Default Server 0 . 0 . 0 . 0

Go To Page 1

| # | Active | Name | Incoming Port(s) | Port Translation | Server IP Address |
|---|---|---|---|---|---|
| 1 | ☑ | FTP | 21 - 21 | 0 - 0 | 192 . 168 . 1 . 39 |
| 2 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 3 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 4 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 5 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 6 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 7 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 8 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 9 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 10 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 11 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |
| 12 | ☐ | | 0 - 0 | 0 - 0 | 0 . 0 . 0 . 0 |

Note 1: You may also need to create a Firewall rule.
Note 2: Port Translation is optional.

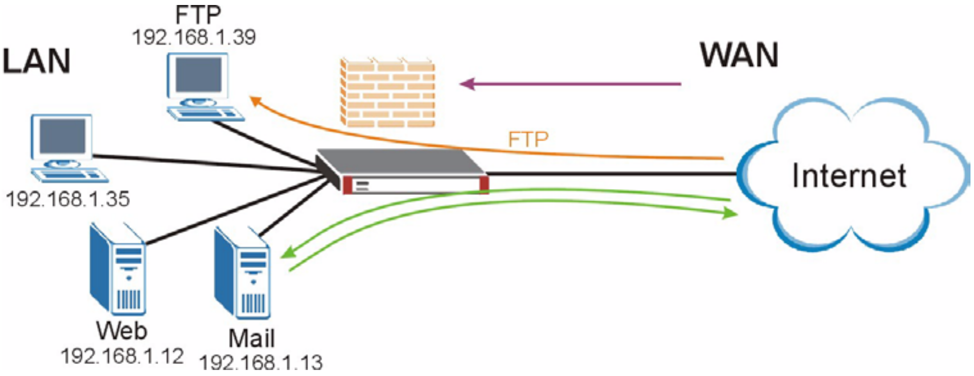
## 4.2.5 Allow WAN-to-LAN Traffic through the Firewall

By default, the ZyWALL blocks any traffic initiated from the WAN to the LAN. To have the ZyWALL forward traffic initiated from the WAN to a local computer or server on the LAN, you need to configure a firewall rule to allow it.

In this example, you create the firewall rules to allow traffic from the WAN to the following servers on the LAN:

- Web server
- Mail server
- FTP server

**Figure 59** Tutorial Example: Forwarding Incoming FTP Traffic to a Local Computer

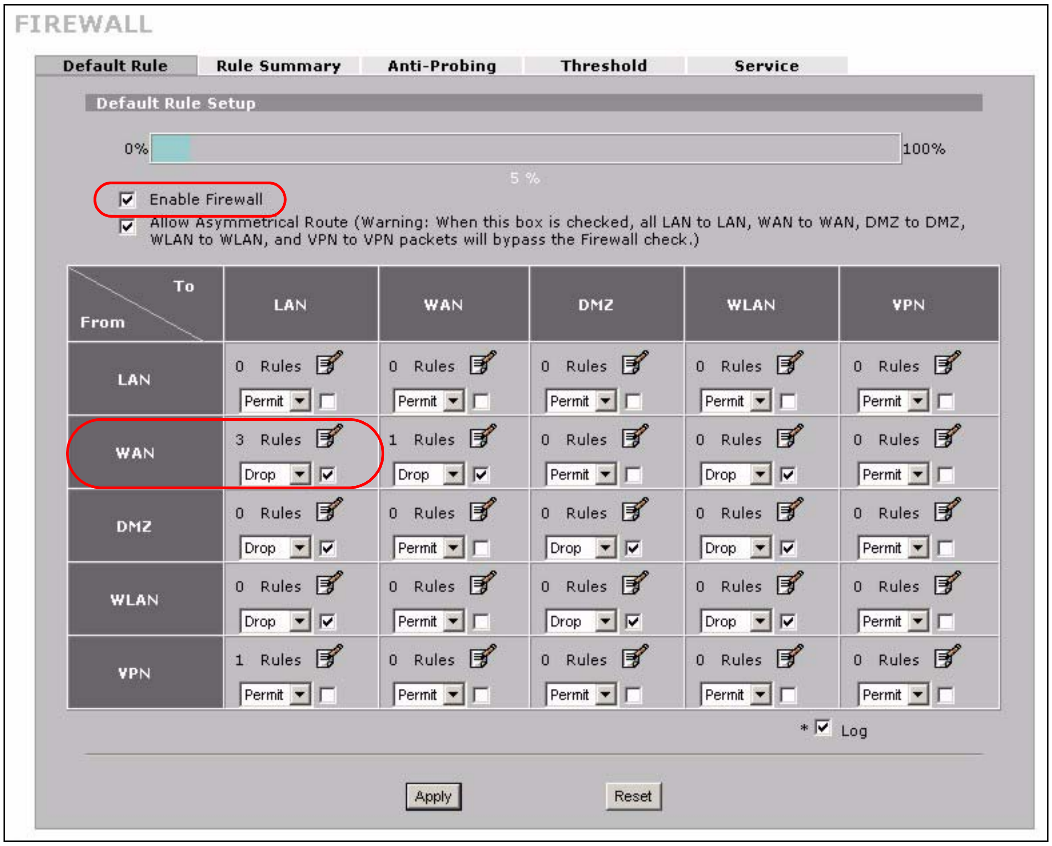


FTP
192.168.1.39
LAN
WAN
FTP
Internet
192.168.1.35
Web
192.168.1.12
Mail
192.168.1.13

1 Click **SECURITY** > **FIREWALL**.

2 Make sure the firewall is enabled and traffic from the WAN to the LAN is dropped.

**Figure 60** Tutorial Example: Firewall Default Rule


FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Default Rule Setup
0%
100%
5 %
Apply
Reset

☑ Enable Firewall

☑ Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ, WLAN to WLAN, and VPN to VPN packets will bypass the Firewall check.)

| From \ To | LAN | WAN | DMZ | WLAN | VPN |
|---|---|---|---|---|---|
| LAN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |
| WAN | 3 Rules<br>Drop ☑ | 1 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| DMZ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| WLAN | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| VPN | 1 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |

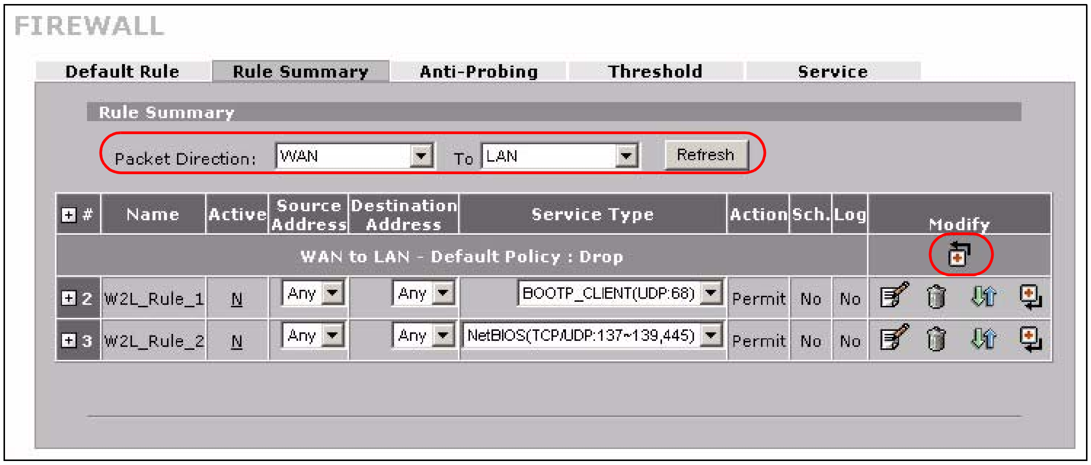
* ☑ Log

**3** Go to the **Rule Summary** screen.

**4** Select **WAN** to **LAN** as the packet direction and click **Refresh**.

**5** Click the insert icon to create a new firewall rule.

**Figure 61** Tutorial Example: Firewall Rule: WAN to LAN


FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Rule Summary
Refresh

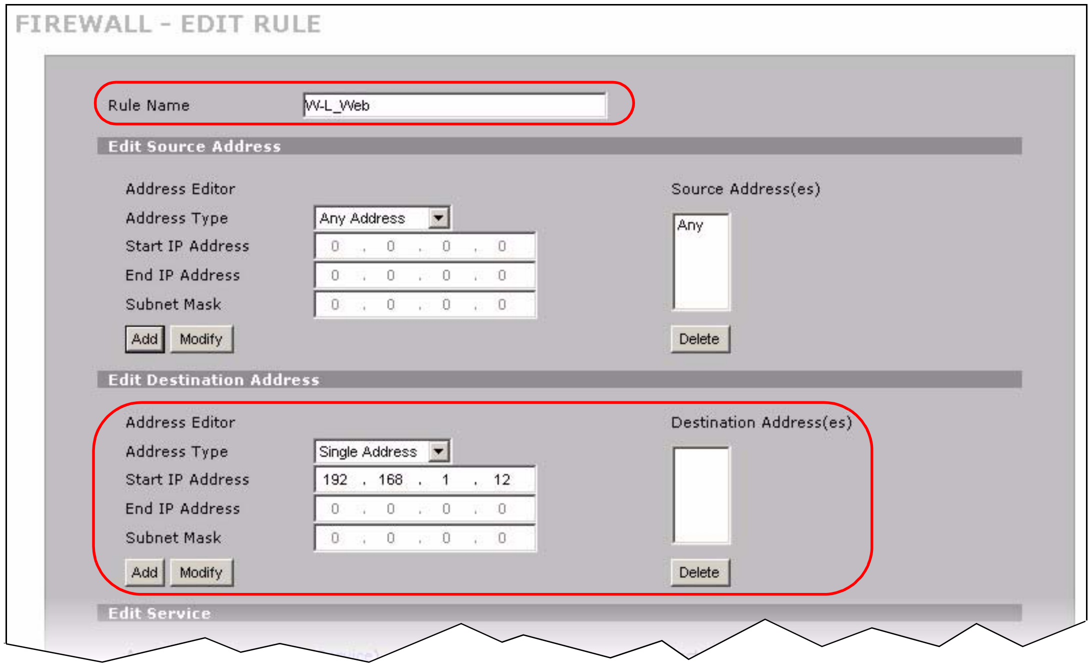
Packet Direction: WAN To LAN

| # | Name | Active | Source Address | Destination Address | Service Type | Action | Sch. | Log | Modify |
|---|---|---|---|---|---|---|---|---|---|
| WAN to LAN - Default Policy : Drop | | | | | | | | | |
| 2 | W2L_Rule_1 | N | Any | Any | BOOTP_CLIENT(UDP:68) | Permit | No | No | |
| 3 | W2L_Rule_2 | N | Any | Any | NetBIOS(TCP/UDP:137~139,445) | Permit | No | No | |

**6** Configure a firewall rule to allow HTTP traffic from the WAN to the web server.

Enter a descriptive name (W-L_Web for example).
Select **Any** in the **Destination Address(es)** box and click **Delete**.
Select **Single Address** as the destination address type. Enter 192.168.1.12 and click **Add**.

**Figure 62** Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Web Server



FIREWALL - EDIT RULE

Rule Name: W-L_Web

Edit Source Address

Address Editor
Address Type: Any Address
Start IP Address: 0 . 0 . 0 . 0
End IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

Source Address(es): Any

Edit Destination Address

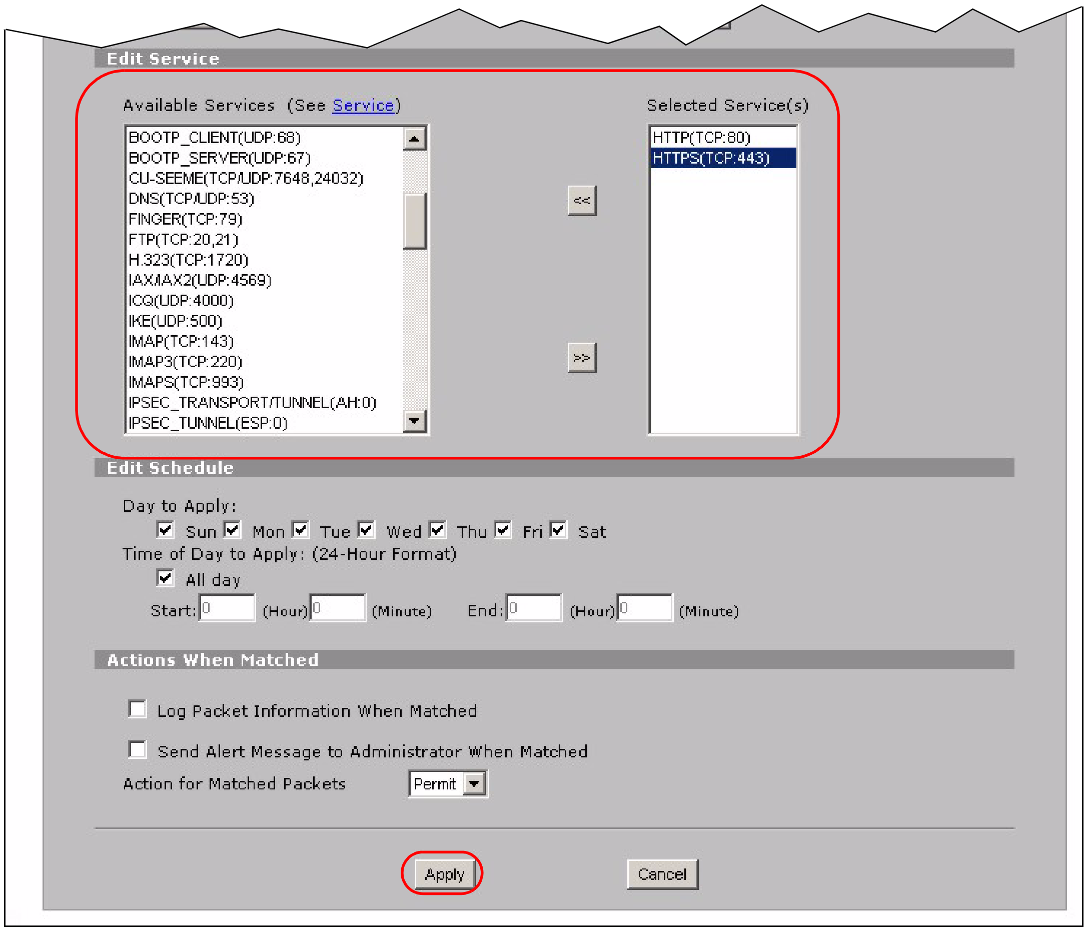
Address Editor
Address Type: Single Address
Start IP Address: 192 . 168 . 1 . 12
End IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0

Destination Address(es)

Edit Service

7 Select **HTTP(TCP:80)** and **HTTPS(TCP:443)** in the **Available Services** box on the left, and click >> to add them to the **Selected Service(s)** box on the right. Click **Apply**.

**Figure 63** Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Web Server



**Edit Service**

Available Services (See Service)

BOOTP_CLIENT(UDP:68)
BOOTP_SERVER(UDP:67)
CU-SEEME(TCP/UDP:7648,24032)
DNS(TCP/UDP:53)
FINGER(TCP:79)
FTP(TCP:20,21)
H.323(TCP:1720)
IAX/IAX2(UDP:4569)
ICQ(UDP:4000)
IKE(UDP:500)
IMAP(TCP:143)
IMAP3(TCP:220)
IMAPS(TCP:993)
IPSEC_TRANSPORT/TUNNEL(AH:0)
IPSEC_TUNNEL(ESP:0)

Selected Service(s)

HTTP(TCP:80)
HTTPS(TCP:443)

**Edit Schedule**

Day to Apply:
☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat
Time of Day to Apply: (24-Hour Format)
☑ All day
Start: 0 (Hour) 0 (Minute) End: 0 (Hour) 0 (Minute)

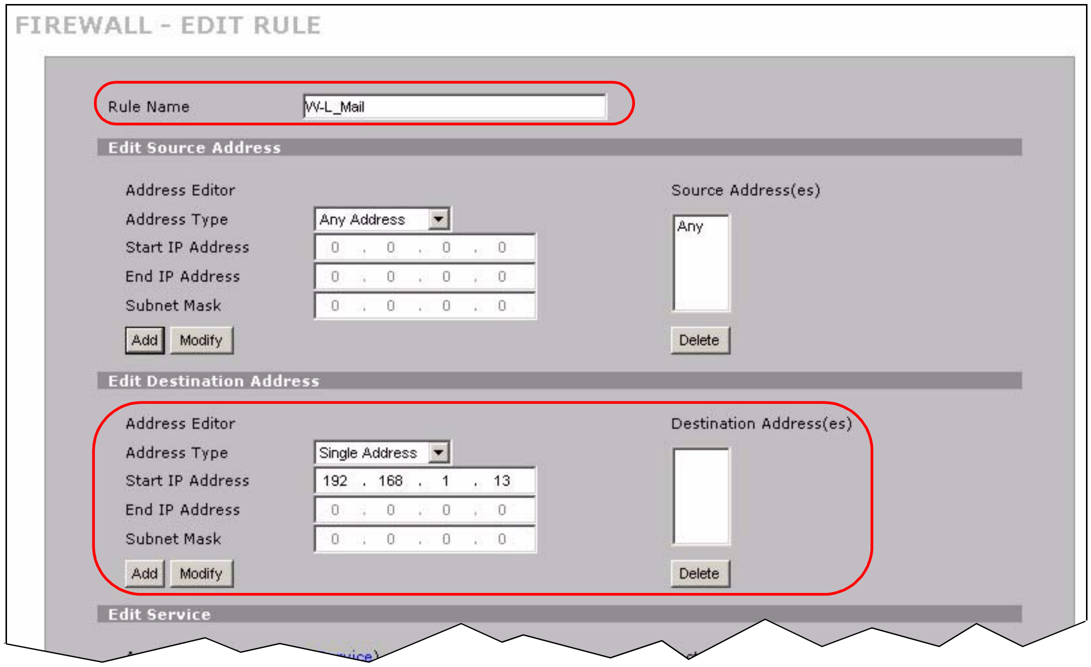
**Actions When Matched**

☐ Log Packet Information When Matched
☐ Send Alert Message to Administrator When Matched
Action for Matched Packets: Permit

**8** Click the insert icon to configure a firewall rule to allow traffic from the WAN to the mail server.

Enter a descriptive name (W-L_Mail for example).
Select **Any** in the **Destination Address(es)** box and click **Delete**.
Select **Single Address** as the destination address type. Enter 192.168.1.13 and click **Add**.

**Figure 64** Tutorial Example: Firewall Rule: WAN to LAN Address Edit for Mail Server



FIREWALL - EDIT RULE

Rule Name: W-L_Mail

Edit Source Address

Address Editor

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Source Address(es): Any

Edit Destination Address

Address Editor

Address Type: Single Address

Start IP Address: 192 . 168 . 1 . 13

End IP Address: 0 . 0 . 0 . 0

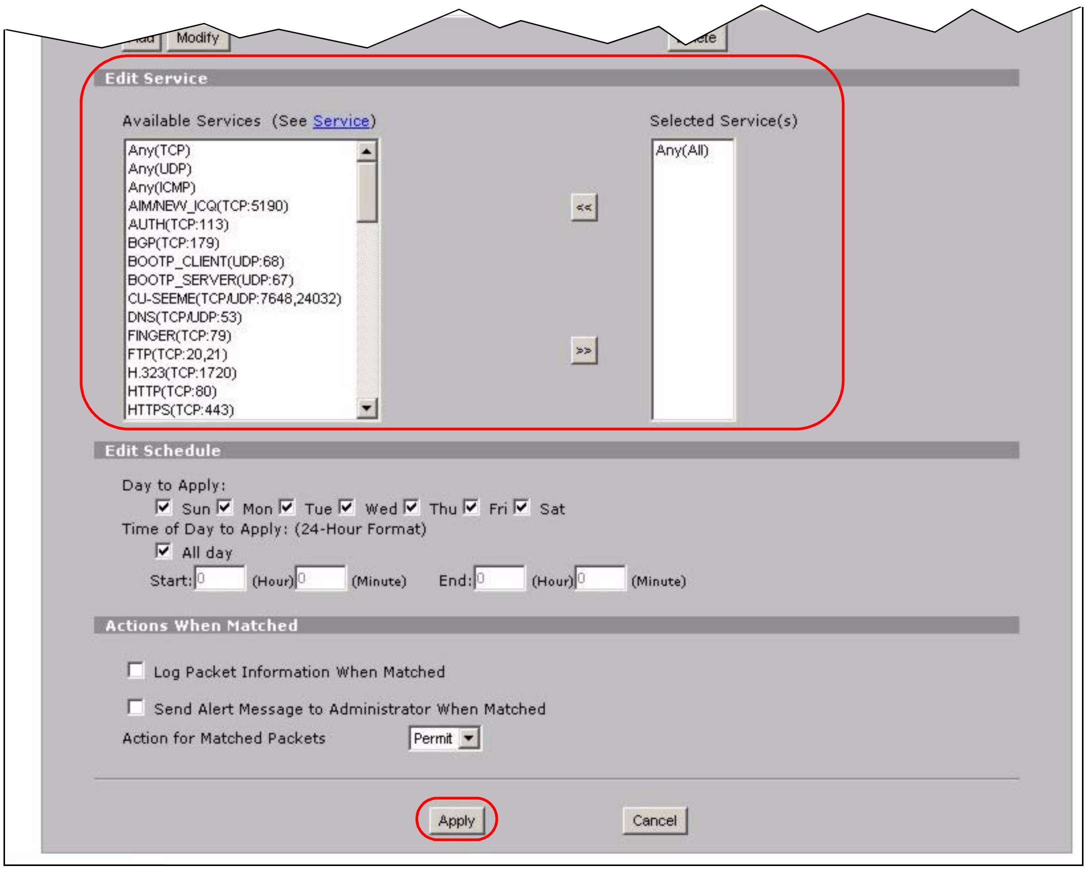
Subnet Mask: 0 . 0 . 0 . 0

Destination Address(es)

Edit Service

**9** Select **Any(All)** in the **Available Services** box on the left, and click >> to add it to the **Selected Service(s)** box on the right. Click **Apply**.

**Figure 65** Tutorial Example: Firewall Rule: WAN to LAN Service Edit for Mail Server



Edit Service

Available Services (See Service)

Any(TCP)
Any(UDP)
Any(ICMP)
AIM/NEW_ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)
BOOTP_CLIENT(UDP:68)
BOOTP_SERVER(UDP:67)
CU-SEEME(TCP/UDP:7648,24032)
DNS(TCP/UDP:53)
FINGER(TCP:79)
FTP(TCP:20,21)
H.323(TCP:1720)
HTTP(TCP:80)
HTTPS(TCP:443)

Selected Service(s): Any(All)

Edit Schedule

Day to Apply:
☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Apply: (24-Hour Format)
☑ All day

Start: 0 (Hour) 0 (Minute) End: 0 (Hour) 0 (Minute)

Actions When Matched

☐ Log Packet Information When Matched

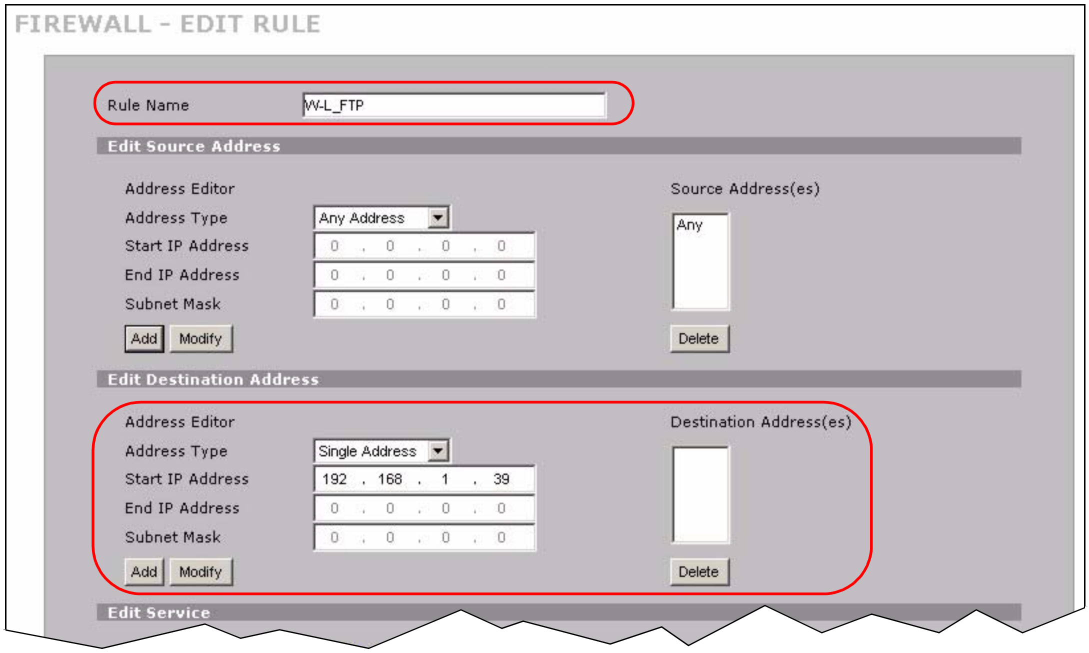
☐ Send Alert Message to Administrator When Matched

Action for Matched Packets: Permit

**10** Click the insert icon to configure a firewall rule to allow FTP traffic from the WAN to the FTP server.

Enter a descriptive name (W-L_FTP for example).
Select **Any** in the **Destination Address(es)** box and click **Delete**.
Select **Single Address** as the destination address type. Enter 192.168.1.39 and click **Add**.

**Figure 66** Tutorial Example: Firewall Rule: WAN to LAN Address Edit for FTP Server



FIREWALL - EDIT RULE

Rule Name: W-L_FTP

Edit Source Address

Address Editor
Address Type: Any Address
Start IP Address: 0 . 0 . 0 . 0
End IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Source Address(es): Any

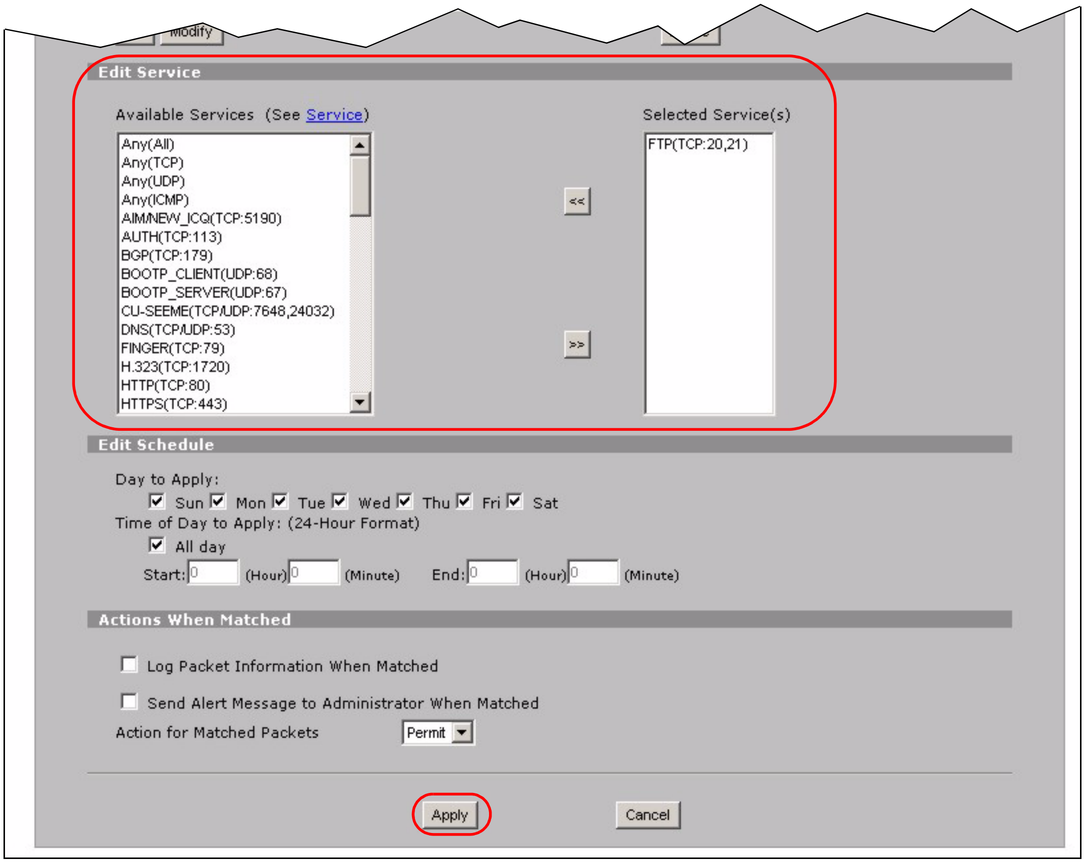
Edit Destination Address

Address Editor
Address Type: Single Address
Start IP Address: 192 . 168 . 1 . 39
End IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Destination Address(es):

Edit Service

**11** Select **FTP(TCP:20,21)** in the **Available Services** box on the left, and click >> to add it to the **Selected Service(s)** box on the right. Click **Apply**.

**Figure 67** Tutorial Example: Firewall Rule: WAN to LAN Service Edit for FTP Server



**Edit Service**

Available Services (See Service)

- Any(All)
- Any(TCP)
- Any(UDP)
- Any(ICMP)
- AIM/NEW_ICQ(TCP:5190)
- AUTH(TCP:113)
- BGP(TCP:179)
- BOOTP_CLIENT(UDP:68)
- BOOTP_SERVER(UDP:67)
- CU-SEEME(TCP/UDP:7648,24032)
- DNS(TCP/UDP:53)
- FINGER(TCP:79)
- H.323(TCP:1720)
- HTTP(TCP:80)
- HTTPS(TCP:443)

Selected Service(s)

- FTP(TCP:20,21)

**Edit Schedule**

Day to Apply:

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Apply: (24-Hour Format)

☑ All day

Start: 0 (Hour) 0 (Minute) End: 0 (Hour) 0 (Minute)

**Actions When Matched**

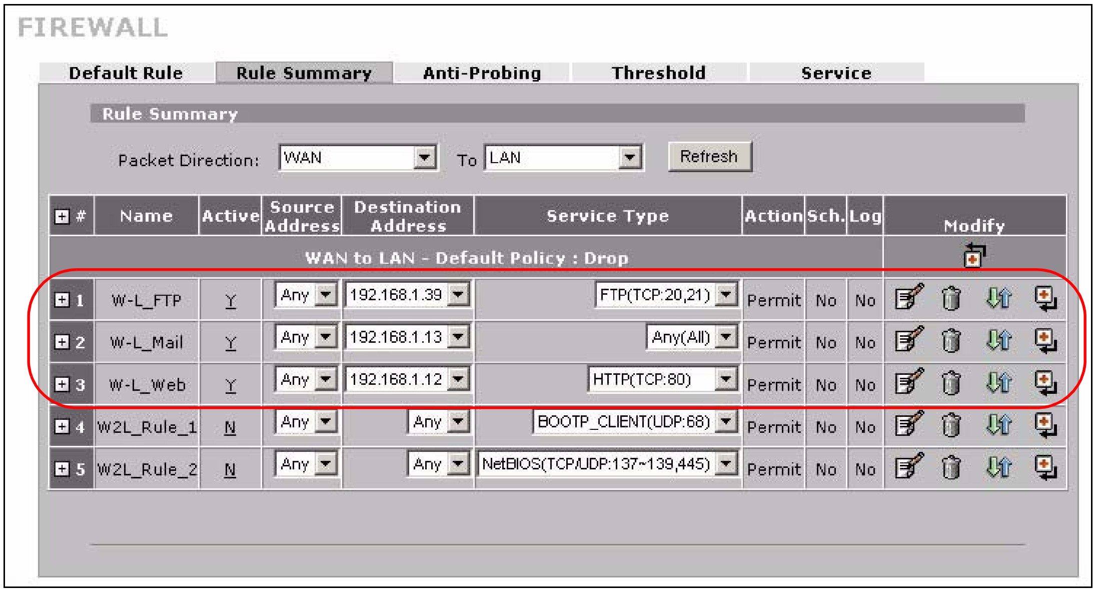
☐ Log Packet Information When Matched

☐ Send Alert Message to Administrator When Matched

Action for Matched Packets: Permit

**12** When you are done, the **Rule Summary** screen looks as shown.

**Figure 68** Tutorial Example: Firewall Rule Summary



**Rule Summary**

Packet Direction: WAN To LAN

| # | Name | Active | Source Address | Destination Address | Service Type | Action | Sch. | Log | Modify |
|---|---|---|---|---|---|---|---|---|---|
| WAN to LAN - Default Policy : Drop | | | | | | | | | |
| 1 | W-L_FTP | Y | Any | 192.168.1.39 | FTP(TCP:20,21) | Permit | No | No | |
| 2 | W-L_Mail | Y | Any | 192.168.1.13 | Any(All) | Permit | No | No | |
| 3 | W-L_Web | Y | Any | 192.168.1.12 | HTTP(TCP:80) | Permit | No | No | |
| 4 | W2L_Rule_1 | N | Any | Any | BOOTP_CLIENT(UDP:68) | Permit | No | No | |
| 5 | W2L_Rule_2 | N | Any | Any | NetBIOS(TCP/UDP:137~139,445) | Permit | No | No | |

### 4.2.6 Testing the Connections

1. Open the web browser on one of the local computers and enter any web site's URL in the address bar. If you can access the web site, your WAN connection and NAT address mapping are configured successfully. If you cannot access it, make sure you entered the correct information in the **WAN** and **NAT Address Mapping** screens. Also check that the Internet account is active and the computer's IP address is in the same subnet as the ZyWALL.
2. Open your web browser and try accessing the web server (1.2.3.5) from the outside network. If you cannot access the web server, make sure the NAT address mapping rule is configured correctly and there is a firewall rule to allow HTTP traffic from the WAN to the web server.
3. Try accessing the FTP server (1.2.3.4) from the outside network to send or retrieve a file. If you cannot access the FTP server, make sure the NAT port forwarding rule is active and there is a firewall rule to allow FTP traffic from the WAN to FTP server.

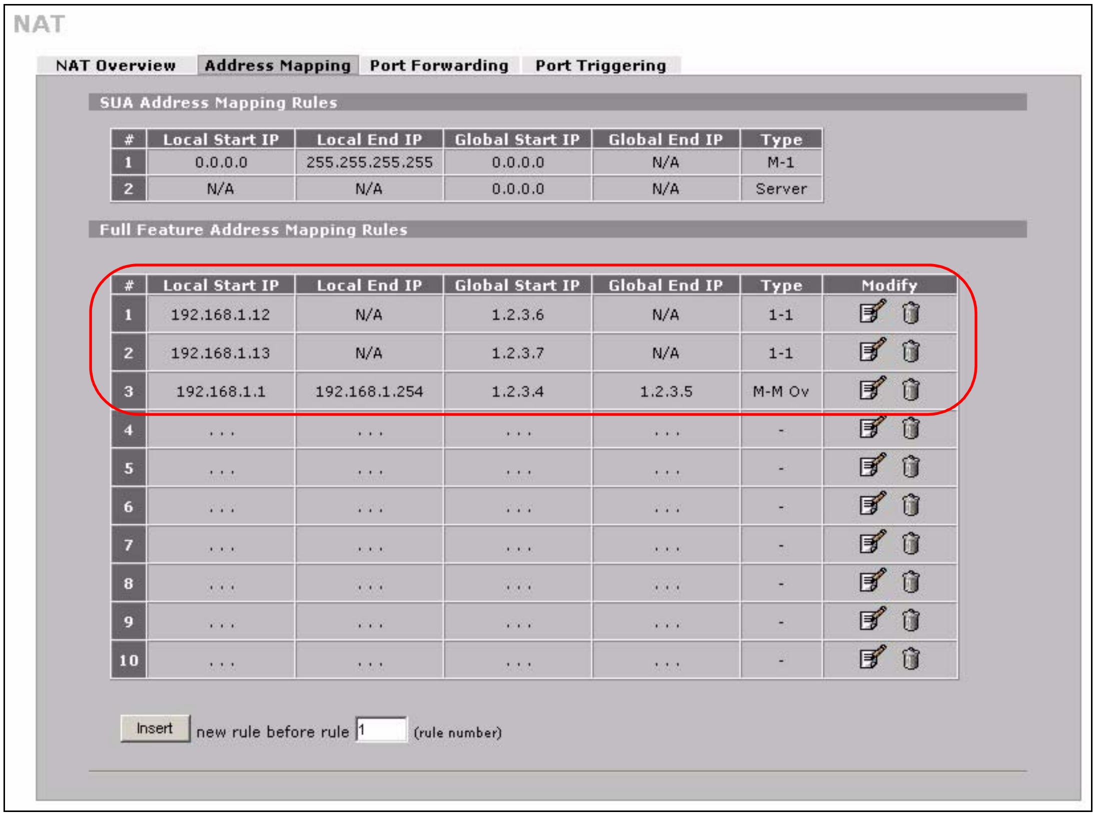
## 4.3 Using NAT with Multiple Game Players

If two users (behind the ZyWALL) want to connect to the same server to play online games at the same time, but the server does not allow more than one login from the same IP address, you can configure a many-to-many rule instead of a many-to-one rule.

In this example, you have four static IP addresses (1.2.3.4 to 1.2.3.7) from your ISP. After you set up your WAN connection (see Section 4.2.2 on page 98), use the **NAT > Address Mapping** screen to map the third and forth public IP addresses to the mail server (192.168.1.12) and web server (192.168.1.13) respectively. The first and second public IP addresses are mapped to other outgoing LAN traffic. See Section 4.2.3 on page 101 for more information about IP address mapping.

When you finish configuration, the screen looks as shown.

**Figure 69** Tutorial Example: NAT Address Mapping Done: Game Playing



SUA Address Mapping Rules

| # | Local Start IP | Local End IP | Global Start IP | Global End IP | Type |
|---|---|---|---|---|---|
| 1 | 0.0.0.0 | 255.255.255.255 | 0.0.0.0 | N/A | M-1 |
| 2 | N/A | N/A | 0.0.0.0 | N/A | Server |

Full Feature Address Mapping Rules

| # | Local Start IP | Local End IP | Global Start IP | Global End IP | Type | Modify |
|---|---|---|---|---|---|---|
| 1 | 192.168.1.12 | N/A | 1.2.3.6 | N/A | 1-1 | ✎ 🗑 |
| 2 | 192.168.1.13 | N/A | 1.2.3.7 | N/A | 1-1 | ✎ 🗑 |
| 3 | 192.168.1.1 | 192.168.1.254 | 1.2.3.4 | 1.2.3.5 | M-M Ov | ✎ 🗑 |
| 4 | ... | ... | ... | ... | - | ✎ 🗑 |
| 5 | ... | ... | ... | ... | - | ✎ 🗑 |
| 6 | ... | ... | ... | ... | - | ✎ 🗑 |
| 7 | ... | ... | ... | ... | - | ✎ 🗑 |
| 8 | ... | ... | ... | ... | - | ✎ 🗑 |
| 9 | ... | ... | ... | ... | - | ✎ 🗑 |
| 10 | ... | ... | ... | ... | - | ✎ 🗑 |

new rule before rule 1 (rule number)

To allow traffic from the WAN to be forwarded through the ZyXEL Device, you must also create a firewall rule. Refer to Section 4.2.5 on page 107 for more information.

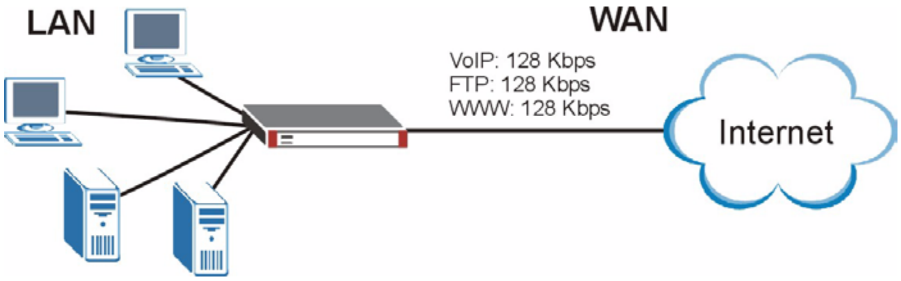
## 4.4 How to Manage the ZyWALL's Bandwidth

This section shows you examples of how to allocate bandwidth and apply priorities to traffic that flows out through the ZyWALL's WAN port.

### 4.4.1 Example Parameters and Scenario

The following figure shows the network you want to set up in this example. The WAN port has an upstream (outgoing) speed of 512 kbps. To prevent SIP-based VoIP (Voice over IP) traffic from getting delayed due to heavy WWW or FTP traffic, you reserve 128 Kbps of bandwidth for outgoing VoIP traffic (from LAN to WAN) and higher priority than FTP or WWW traffic.

**Figure 70** Tutorial Example: Bandwidth Management



The following table shows the example information you configure in the bandwidth management screens.

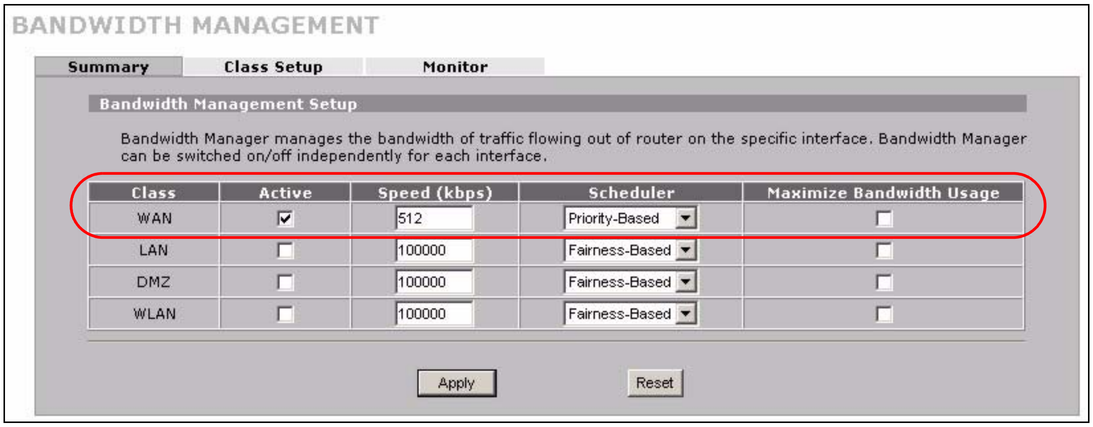
| | |
|---|---|
| **Total Bandwidth Budget (WAN Upstream Speed)** | 512 Kbps |
| **Bandwidth for VoIP Traffic** | 128 Kbps |
| **Priority for VoIP Traffic** | 7 |
| **Bandwidth for FTP Traffic** | 128 Kbps |
| **Priority for FTP Traffic** | 2 |
| **Bandwidth for WWW Traffic** | 128 Kbps |
| **Priority for WWW Traffic** | 3 |

## 4.4.2 Configuring Bandwidth Management Rules

Follow the steps below to set up bandwidth management rules for different traffic.

1. Click **ADVANCED** > **BW MGMT**.
2. Select **Active** to apply bandwidth management to traffic that is forwarded out through the WAN port.
3. Enter the WAN port's upstream speed.
4. Select **Priority-Based** to have the ZyWALL give preference to bandwidth classes with higher priorities.
5. Deselect the **Maximize Bandwidth Usage** option to reserve bandwidth for traffic that is not defined in a bandwidth class.
6. Click **Apply**.

**Figure 71** Tutorial Example: Bandwidth Management Summary


BANDWIDTH MANAGEMENT
Summary
Class Setup
Monitor
Bandwidth Management Setup
Apply
Reset

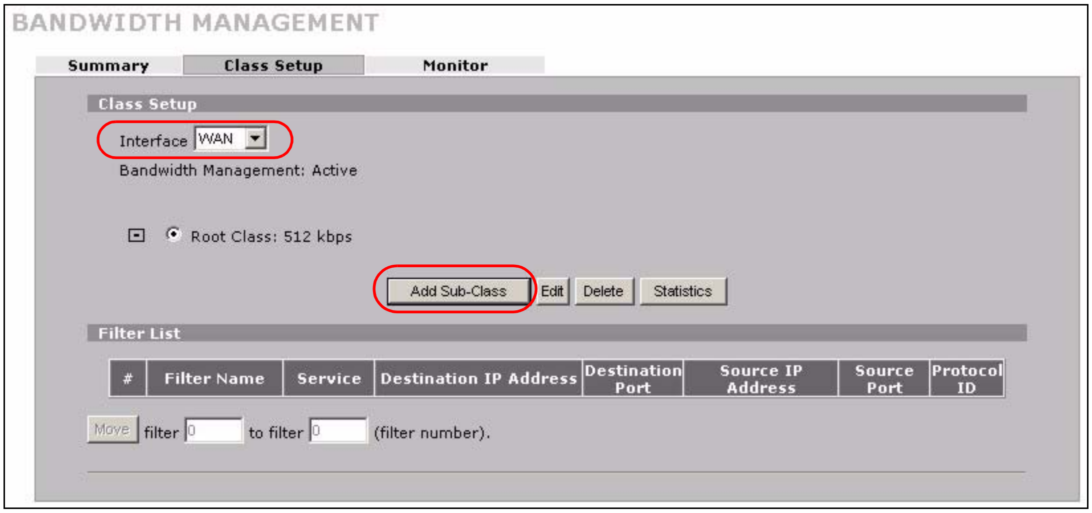
Bandwidth Manager manages the bandwidth of traffic flowing out of router on the specific interface. Bandwidth Manager can be switched on/off independently for each interface.

| Class | Active | Speed (kbps) | Scheduler | Maximize Bandwidth Usage |
|---|---|---|---|---|
| WAN | ☑ | 512 | Priority-Based | ☐ |
| LAN | ☐ | 100000 | Fairness-Based | ☐ |
| DMZ | ☐ | 100000 | Fairness-Based | ☐ |
| WLAN | ☐ | 100000 | Fairness-Based | ☐ |

**7** Click the **Class Setup** tab.

**8** Select the **WAN** interface and click the **Add Sub-Class** button to create a rule for VoIP traffic.

**Figure 72** Tutorial Example: Bandwidth Management Class Setup


BANDWIDTH MANAGEMENT
Summary
Class Setup
Monitor
Class Setup
Add Sub-Class
Edit
Delete
Statistics
Filter List
Move

Interface WAN

Bandwidth Management: Active

● Root Class: 512 kbps

| # | Filter Name | Service | Destination IP Address | Destination Port | Source IP Address | Source Port | Protocol ID |
|---|---|---|---|---|---|---|---|

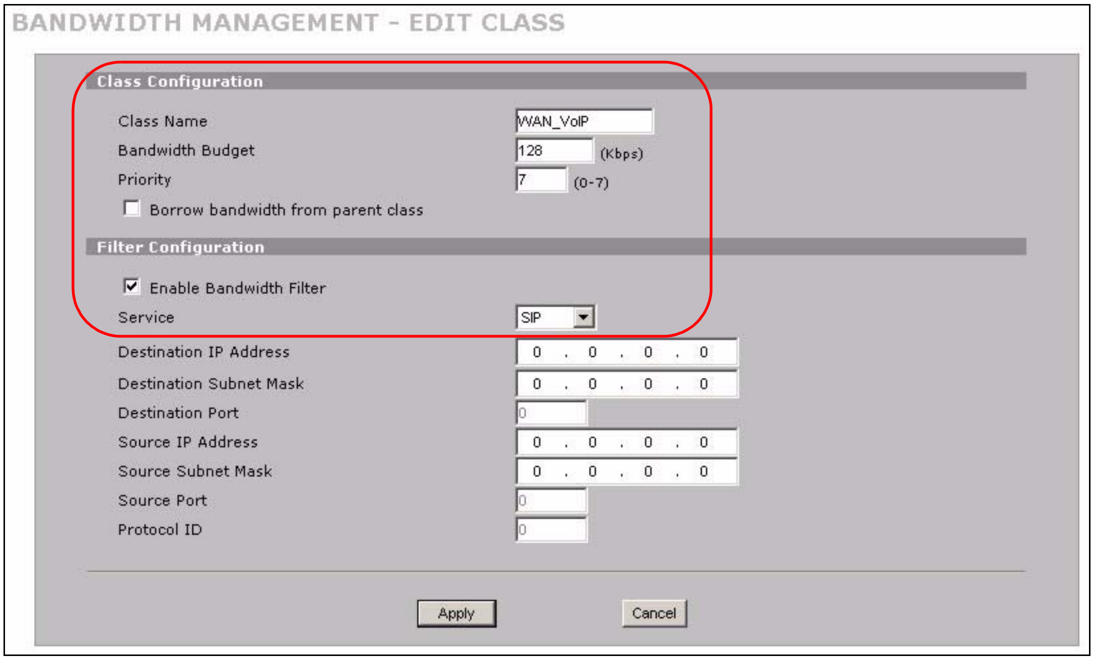
filter 0 to filter 0 (filter number).

**9** Enter a descriptive name (WAN_VoIP for example), the maximum bandwidth allowed and a priority for VoIP traffic. The higher the number, the higher the priority.

**10** Enable this filter and select the SIP service.

**11** Leave the IP address and subnet mask fields blank, so that the filter will be applied to any outgoing traffic through the WAN port. Click **Apply**.

**Figure 73** Tutorial Example: Bandwidth Management Class Setup: VoIP


BANDWIDTH MANAGEMENT - EDIT CLASS

Class Configuration

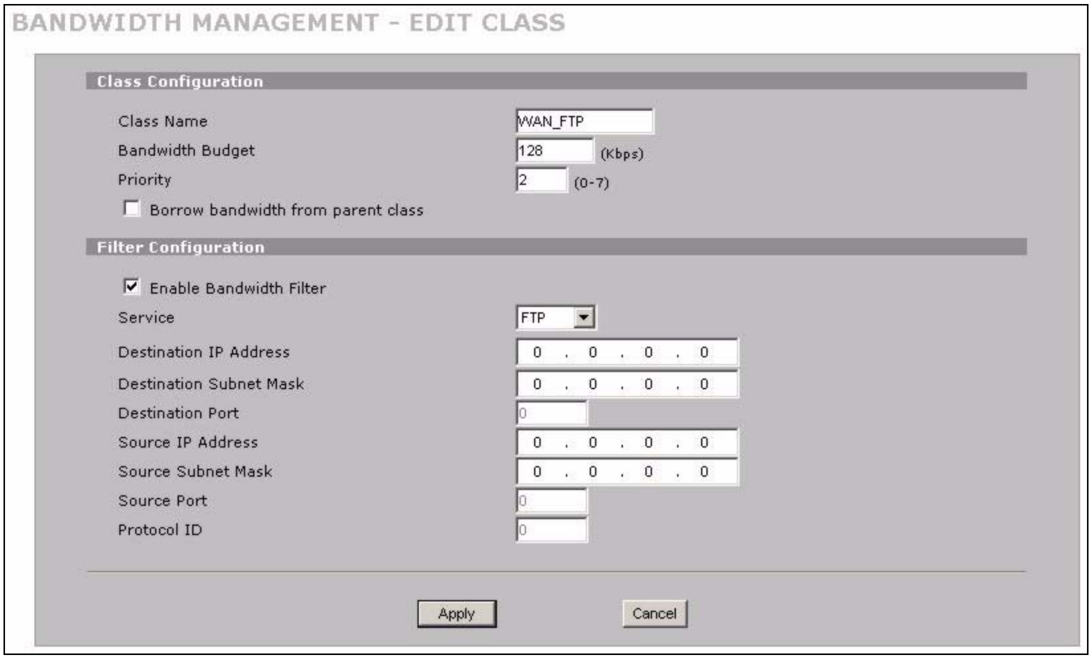
| | |
|---|---|
| Class Name | WAN_VoIP |
| Bandwidth Budget | 128 (Kbps) |
| Priority | 7 (0-7) |
| ☐ Borrow bandwidth from parent class | |

Filter Configuration

| | |
|---|---|
| ☑ Enable Bandwidth Filter | |
| Service | SIP |
| Destination IP Address | 0 . 0 . 0 . 0 |
| Destination Subnet Mask | 0 . 0 . 0 . 0 |
| Destination Port | 0 |
| Source IP Address | 0 . 0 . 0 . 0 |
| Source Subnet Mask | 0 . 0 . 0 . 0 |
| Source Port | 0 |
| Protocol ID | 0 |

**12** Click the **Add Sub-Class** button to create a rule for FTP traffic as follows. Click **Apply**.

**Figure 74** Tutorial Example: Bandwidth Management Class Setup: FTP


BANDWIDTH MANAGEMENT - EDIT CLASS

Class Configuration

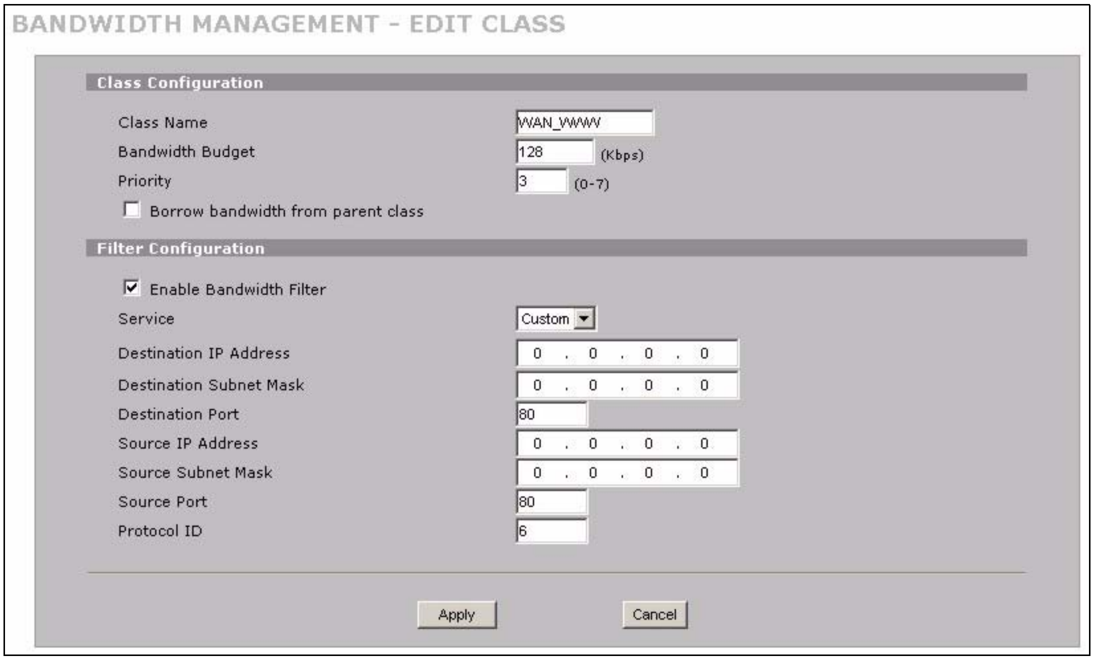
| | |
|---|---|
| Class Name | WAN_FTP |
| Bandwidth Budget | 128 (Kbps) |
| Priority | 2 (0-7) |
| ☐ Borrow bandwidth from parent class | |

Filter Configuration

| | |
|---|---|
| ☑ Enable Bandwidth Filter | |
| Service | FTP |
| Destination IP Address | 0 . 0 . 0 . 0 |
| Destination Subnet Mask | 0 . 0 . 0 . 0 |
| Destination Port | 0 |
| Source IP Address | 0 . 0 . 0 . 0 |
| Source Subnet Mask | 0 . 0 . 0 . 0 |
| Source Port | 0 |
| Protocol ID | 0 |

**13** Click the **Add Sub-Class** button to create a rule for WWW traffic as follows. Click **Apply**.

**Figure 75** Tutorial Example: Bandwidth Management Class Setup: WWW



BANDWIDTH MANAGEMENT - EDIT CLASS

Class Configuration

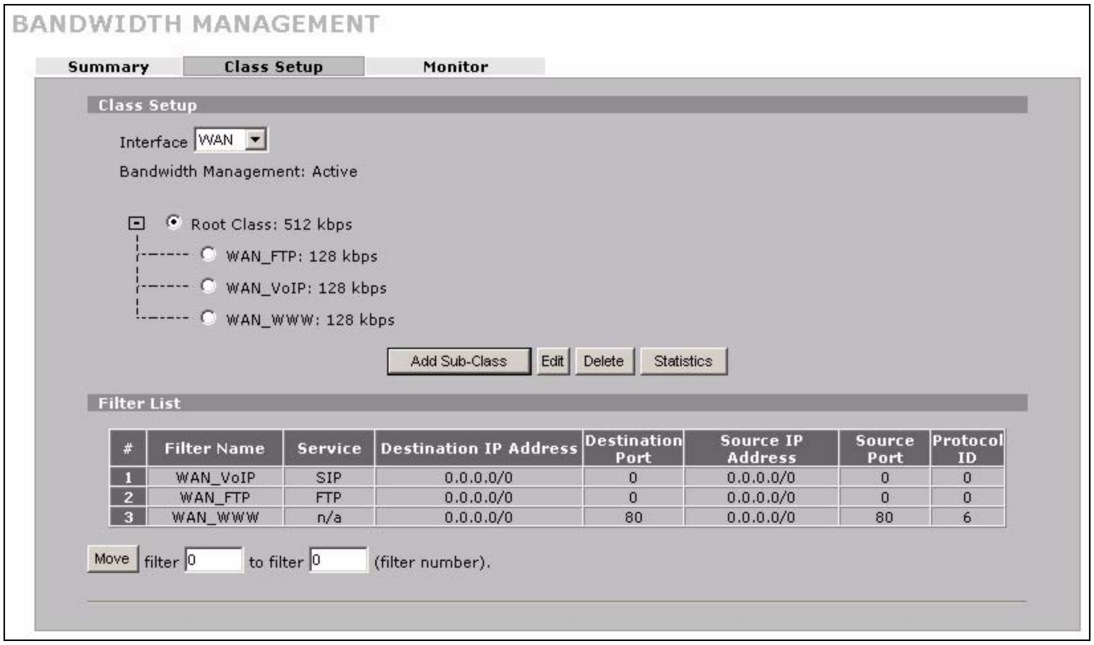
Class Name: WAN_WWW
Bandwidth Budget: 128 (Kbps)
Priority: 3 (0-7)
☐ Borrow bandwidth from parent class

Filter Configuration

☑ Enable Bandwidth Filter
Service: Custom
Destination IP Address: 0 . 0 . 0 . 0
Destination Subnet Mask: 0 . 0 . 0 . 0
Destination Port: 80
Source IP Address: 0 . 0 . 0 . 0
Source Subnet Mask: 0 . 0 . 0 . 0
Source Port: 80
Protocol ID: 6

**14** When you are finished, the **Class Setup** screen looks as shown.

**Figure 76** Tutorial Example: Bandwidth Management Class Setup Done



Class Setup

Interface: WAN
Bandwidth Management: Active

● Root Class: 512 kbps
○ WAN_FTP: 128 kbps
○ WAN_VoIP: 128 kbps
○ WAN_WWW: 128 kbps

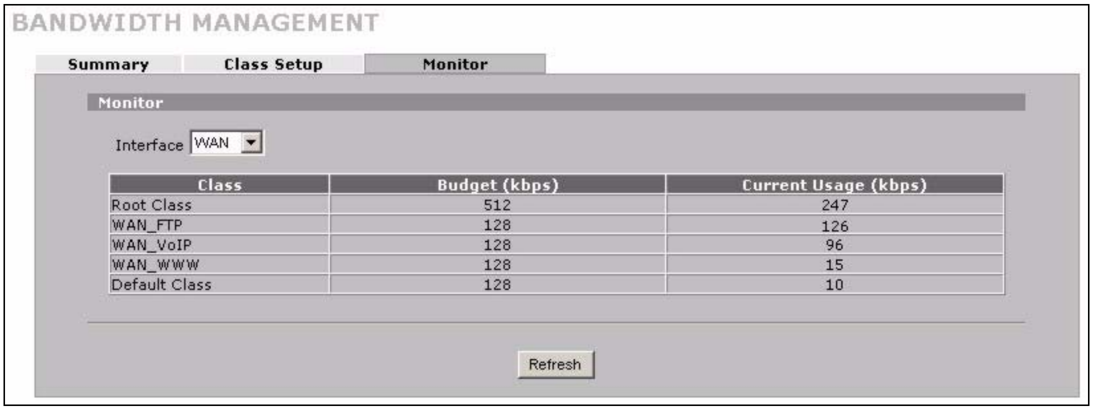
Filter List

| # | Filter Name | Service | Destination IP Address | Destination Port | Source IP Address | Source Port | Protocol ID |
|---|---|---|---|---|---|---|---|
| 1 | WAN_VoIP | SIP | 0.0.0.0/0 | 0 | 0.0.0.0/0 | 0 | 0 |
| 2 | WAN_FTP | FTP | 0.0.0.0/0 | 0 | 0.0.0.0/0 | 0 | 0 |
| 3 | WAN_WWW | n/a | 0.0.0.0/0 | 80 | 0.0.0.0/0 | 80 | 6 |

Move filter 0 to filter 0 (filter number).

**15** Use the **Monitor** screen to view the bandwidth usage and allotments for the WAN interface.

**Figure 77** Tutorial Example: Bandwidth Management Monitor



Interface WAN

| Class | Budget (kbps) | Current Usage (kbps) |
|---|---|---|
| Root Class | 512 | 247 |
| WAN_FTP | 128 | 126 |
| WAN_VoIP | 128 | 96 |
| WAN_WWW | 128 | 15 |
| Default Class | 128 | 10 |

## 4.5 Configuring Content Filtering

You can use the ZyWALL's content filtering policies to apply specific content filtering settings to specific users. You can even filter certain things at certain times. For example, you decide to set the default policy to block access to several categories of web content including things like pornography, hacking, nudity, and arts and entertainment, and so on. Now, suppose you want to allow an employee named Bob to access arts and entertainment web pages during lunch. You can create another policy for traffic from Bob's computer.

The ordering of your policies is very important as the ZyWALL applies policies in the order they are listed.

The ZyWALL applies the content filter policies based on the source address and the schedule. So for this example, when the ZyWALL receives a request from the LAN for a web page, it checks the request against the first policy. If the traffic matches (that is if it is from Bob's computer and the time is between 12:00 and 13:00), the ZyWALL applies the first policy. Any traffic that does not match the first policy will match the default policy and the ZyWALL treats it based on the default policy.

### 4.5.1 Enable Content Filtering

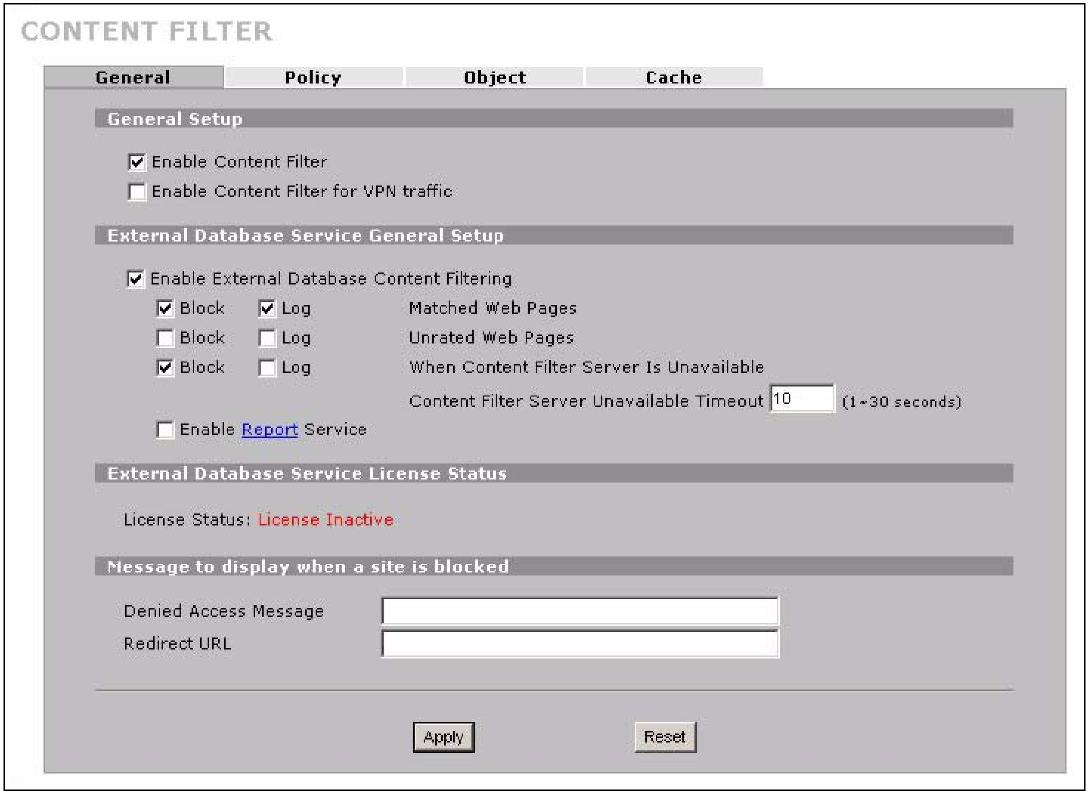
Do the following to turn on content filtering and have the ZyWALL use the external content filtering service.

You must register for external content filtering before you can use it.

Use the **REGISTRATION** screens (see Chapter 5 on page 127) to create a myZyXEL.com account, register your device and activate the external content filtering service.

1 Click **SECURITY** > **CONTENT FILTER**.
2 Enable the content filter and external database content filtering.
3 Click **Apply**.

**Figure 78** SECURITY > CONTENT FILTER > General



General Setup

☑ Enable Content Filter
☐ Enable Content Filter for VPN traffic

External Database Service General Setup

☑ Enable External Database Content Filtering
☑ Block ☑ Log Matched Web Pages
☐ Block ☐ Log Unrated Web Pages
☑ Block ☐ Log When Content Filter Server Is Unavailable
Content Filter Server Unavailable Timeout 10 (1~30 seconds)
☐ Enable Report Service

External Database Service License Status

License Status: License Inactive

Message to display when a site is blocked

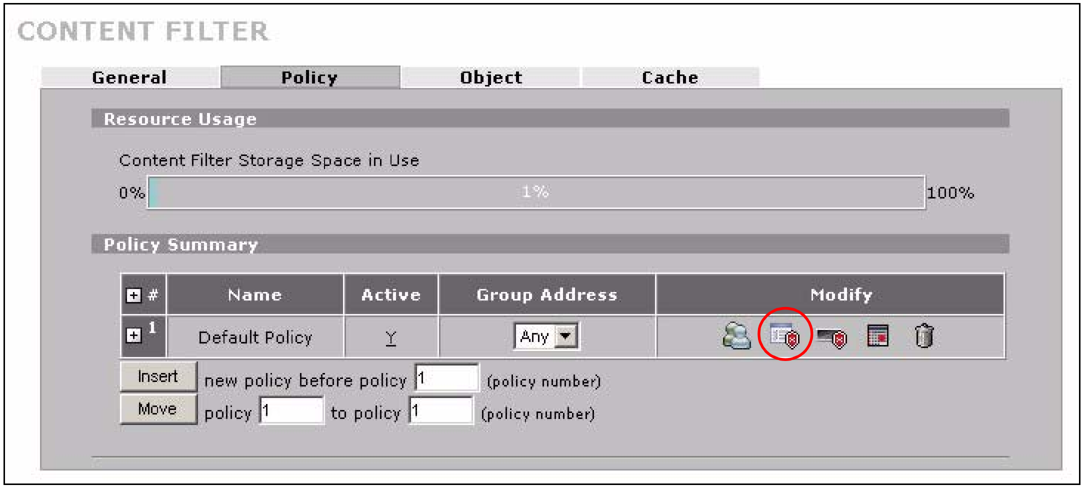
Denied Access Message
Redirect URL

## 4.5.2 Block Categories of Web Content

Here is how to block access to web pages by category of content.

1 Click **SECURITY** > **CONTENT FILTER** > **Policy** and then the external database icon next to the default policy.

**Figure 79** SECURITY > CONTENT FILTER > Policy



CONTENT FILTER

General
Policy
Object
Cache

**Resource Usage**

Content Filter Storage Space in Use

0% 1% 100%

**Policy Summary**

| ⊞ # | Name | Active | Group Address | Modify |
|---|---|---|---|---|
| ⊞ 1 | Default Policy | Y | Any | |

Insert
new policy before policy 1 (policy number)

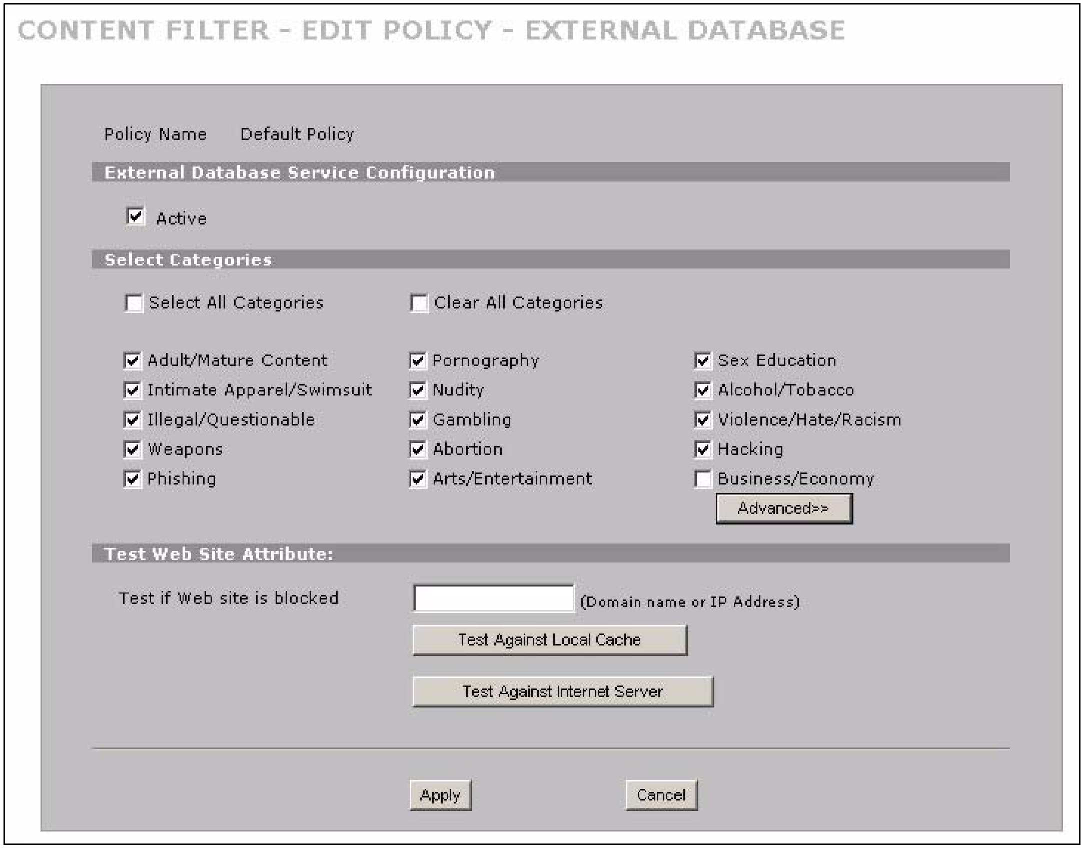
Move
policy 1 to policy 1 (policy number)

2 Select **Active**.

3 Select the categories to block.

4 Click **Apply**.

**Figure 80** SECURITY > CONTENT FILTER > Policy > External Database (Default)



CONTENT FILTER - EDIT POLICY - EXTERNAL DATABASE

Policy Name Default Policy

**External Database Service Configuration**

☑ Active

**Select Categories**

☐ Select All Categories ☐ Clear All Categories

☑ Adult/Mature Content
☑ Intimate Apparel/Swimsuit
☑ Illegal/Questionable
☑ Weapons
☑ Phishing
☑ Pornography
☑ Nudity
☑ Gambling
☑ Abortion
☑ Arts/Entertainment
☑ Sex Education
☑ Alcohol/Tobacco
☑ Violence/Hate/Racism
☑ Hacking
☐ Business/Economy

**Test Web Site Attribute:**

Test if Web site is blocked (Domain name or IP Address)

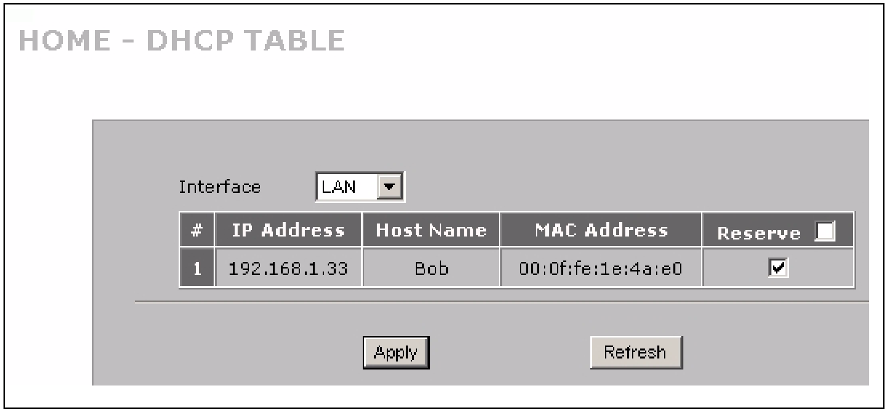
Test Against Local Cache
Test Against Internet Server
Apply
Cancel

### 4.5.3 Assign Bob’s Computer a Specific IP Address

You will configure a content filtering policy for traffic from Bob’s computer’s IP address. Do the following to have the ZyWALL always give Bob’s computer the same IP address (192.168.1.33 in this example).

1. Click **HOME** > **DHCP Table**.
2. Find the entry for Bob’s computer and select the **Reserve** check box as shown next.
3. Click **Apply**.

**Figure 81** HOME > DHCP Table


HOME - DHCP TABLE
Apply
Refresh

Interface: LAN

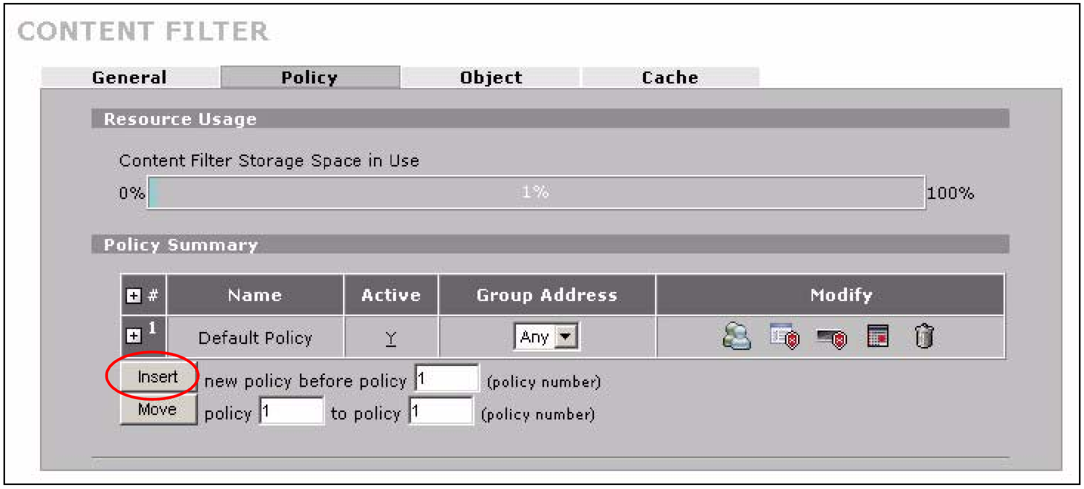
| # | IP Address | Host Name | MAC Address | Reserve ☐ |
|---|---|---|---|---|
| 1 | 192.168.1.33 | Bob | 00:0f:fe:1e:4a:e0 | ☑ |

### 4.5.4 Create a Content Filter Policy for Bob

Do the following to create a content filtering policy for traffic from Bob’s computer.

1. Click **SECURITY** > **CONTENT FILTER** > **Policy** and then the **Insert** button. The ZyWALL applies the content filter policies in order, so make sure you add the new policy before the default policy.

**Figure 82** SECURITY > CONTENT FILTER > Policy


CONTENT FILTER
General
Policy
Object
Cache
Resource Usage
Content Filter Storage Space in Use
0%
1%
100%
Policy Summary
Insert
Move

| # | Name | Active | Group Address | Modify |
|---|---|---|---|---|
| 1 | Default Policy | Y | Any | |

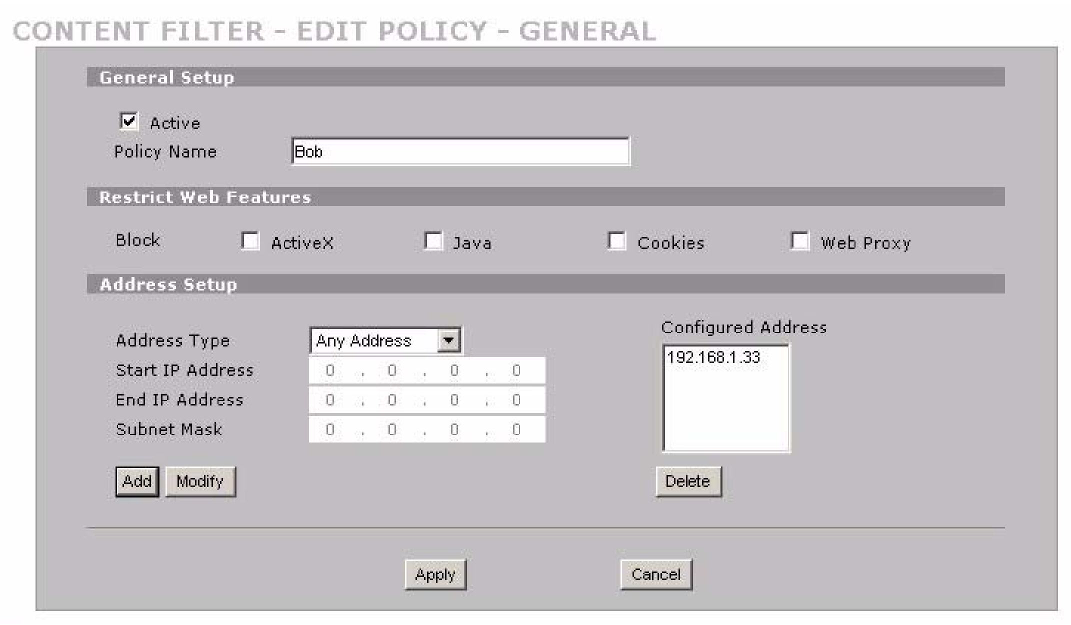
Insert new policy before policy 1 (policy number)

Move policy 1 to policy 1 (policy number)

2. Select **Active**.
3. Give the policy a name.
4. Configure a single address of 192.168.1.33.

**5** Click **Apply**.

**Figure 83** SECURITY > CONTENT FILTER > Policy > Insert


CONTENT FILTER - EDIT POLICY - GENERAL
General Setup
Restrict Web Features
Block
☐ ActiveX
☐ Java
☐ Cookies
☐ Web Proxy
Address Setup
Add
Modify
Delete
Apply
Cancel

☑ Active

Policy Name: Bob

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

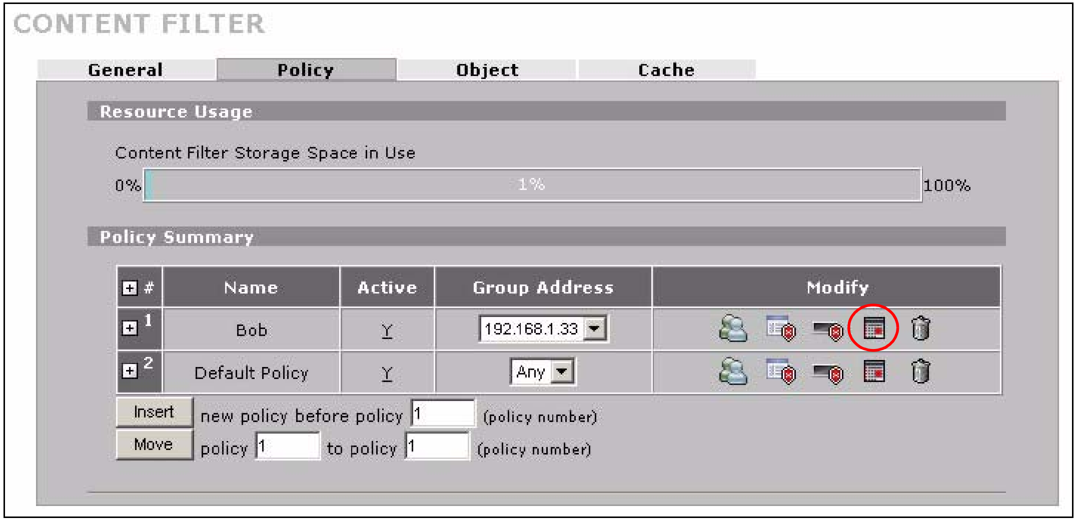
Configured Address: 192.168.1.33

## 4.5.5 Set the Content Filter Schedule

You want to let Bob access arts and entertainment web pages, but only during lunch. So you configure a schedule to only apply the Bob policy from 12:00 to 13:00. For the rest of the time, the ZyWALL applies the default content filter policy (which blocks access to arts and entertainment web pages).

**1** Click **SECURITY** > **CONTENT FILTER** > **Policy** and then the Bob policy’s schedule icon.

**Figure 84** SECURITY > CONTENT FILTER > Policy


CONTENT FILTER
General
Policy
Object
Cache
Resource Usage
Policy Summary
Insert
Move

Content Filter Storage Space in Use: 0% 1% 100%

| # | Name | Active | Group Address | Modify |
|---|---|---|---|---|
| 1 | Bob | Y | 192.168.1.33 | |
| 2 | Default Policy | Y | Any | |

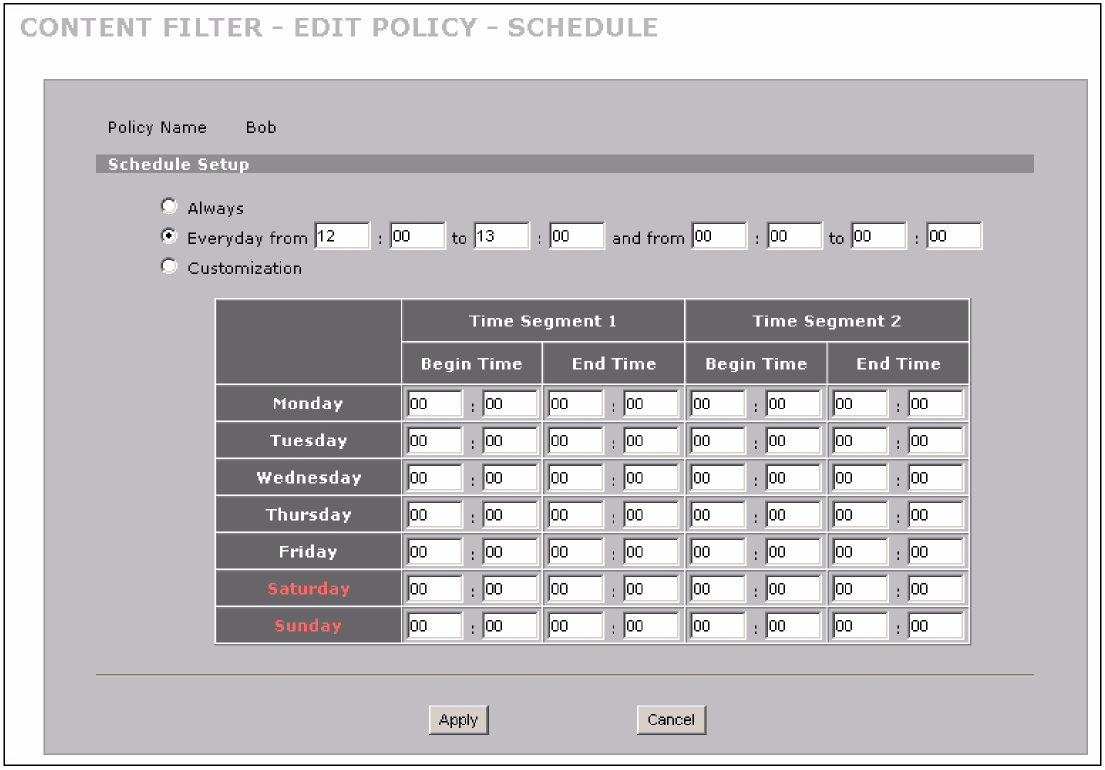
Insert new policy before policy 1 (policy number)

Move policy 1 to policy 1 (policy number)

**2** Select **Everyday** and enter 12:00 to 13:00.

**3** Click **Apply**.

**Figure 85** SECURITY > CONTENT FILTER > Policy > Schedule (Bob)



CONTENT FILTER - EDIT POLICY - SCHEDULE

Policy Name Bob

Schedule Setup

○ Always
● Everyday from 12 : 00 to 13 : 00 and from 00 : 00 to 00 : 00
○ Customization

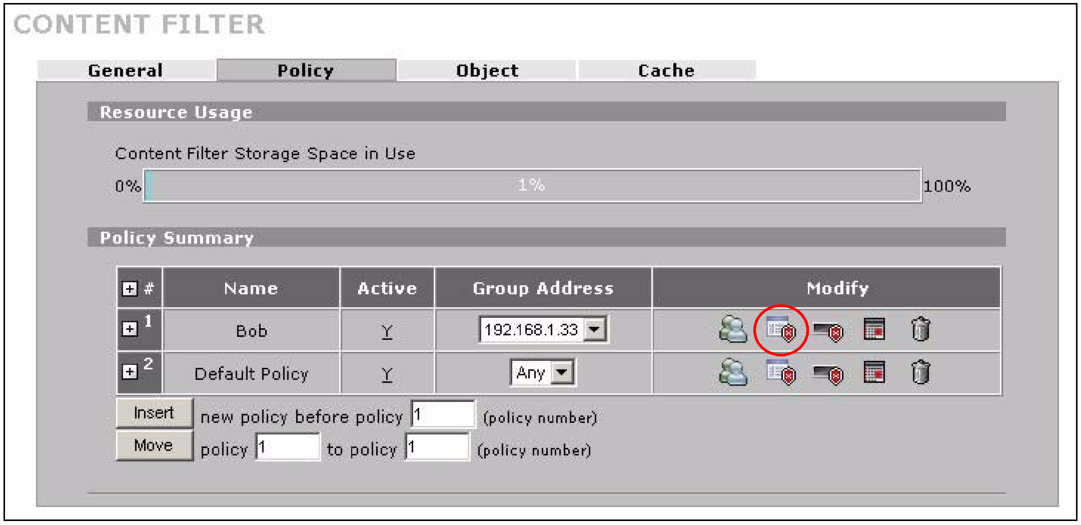
| | Time Segment 1 | | Time Segment 2 | |
|---|---|---|---|---|
| | Begin Time | End Time | Begin Time | End Time |
| Monday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Tuesday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Wednesday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Thursday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Friday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Saturday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Sunday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |

## 4.5.6 Block Categories of Web Content for Bob

Now you select the categories of web pages to block Bob from accessing.

1. Click **SECURITY** > **CONTENT FILTER** > **Policy** and then the Bob policy's external database icon.

**Figure 86** SECURITY > CONTENT FILTER > Policy



CONTENT FILTER

Resource Usage

Content Filter Storage Space in Use

0% 1% 100%

Policy Summary

| # | Name | Active | Group Address | Modify |
|---|---|---|---|---|
| 1 | Bob | Y | 192.168.1.33 | |
| 2 | Default Policy | Y | Any | |

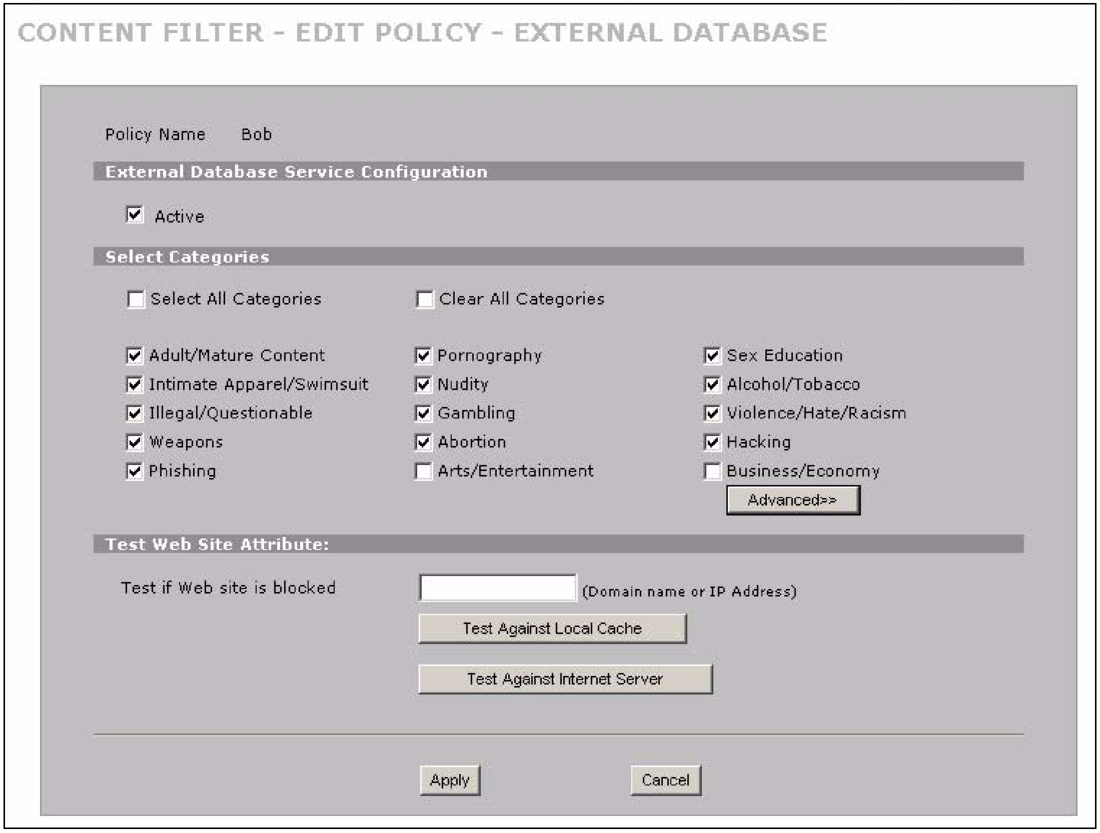
Insert new policy before policy 1 (policy number)

Move policy 1 to policy 1 (policy number)

2. Select **Active**.
3. Select the categories to block. This is very similar to Section 4.5.2 on page 121, except you do not select the arts and entertainment category.

4 Click **Apply**.

**Figure 87** SECURITY > CONTENT FILTER > Policy > External Database (Bob)



CONTENT FILTER - EDIT POLICY - EXTERNAL DATABASE

Policy Name Bob

**External Database Service Configuration**

☑ Active

**Select Categories**

☐ Select All Categories ☐ Clear All Categories

| | | |
|---|---|---|
| ☑ Adult/Mature Content | ☑ Pornography | ☑ Sex Education |
| ☑ Intimate Apparel/Swimsuit | ☑ Nudity | ☑ Alcohol/Tobacco |
| ☑ Illegal/Questionable | ☑ Gambling | ☑ Violence/Hate/Racism |
| ☑ Weapons | ☑ Abortion | ☑ Hacking |
| ☑ Phishing | ☐ Arts/Entertainment | ☐ Business/Economy |

**Test Web Site Attribute:**

Test if Web site is blocked (Domain name or IP Address)

Test Against Local Cache
Test Against Internet Server
Apply
Cancel

# 5

# Registration

## 5.1 myZyXEL.com overview

myZyXEL.com is ZyXEL's online services center where you can register your ZyWALL and manage subscription services available for the ZyWALL.

✍ You need to create an account before you can register your device and activate the services at myZyXEL.com.

You can directly create a myZyXEL.com account, register your ZyWALL and activate a service using the **REGISTRATION** screen. Alternatively, go to http://www.myZyXEL.com with the ZyWALL's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

✍ To activate a service on a ZyWALL, you need to access myZyXEL.com via that ZyWALL.

### 5.1.1 Content Filtering Subscription Service

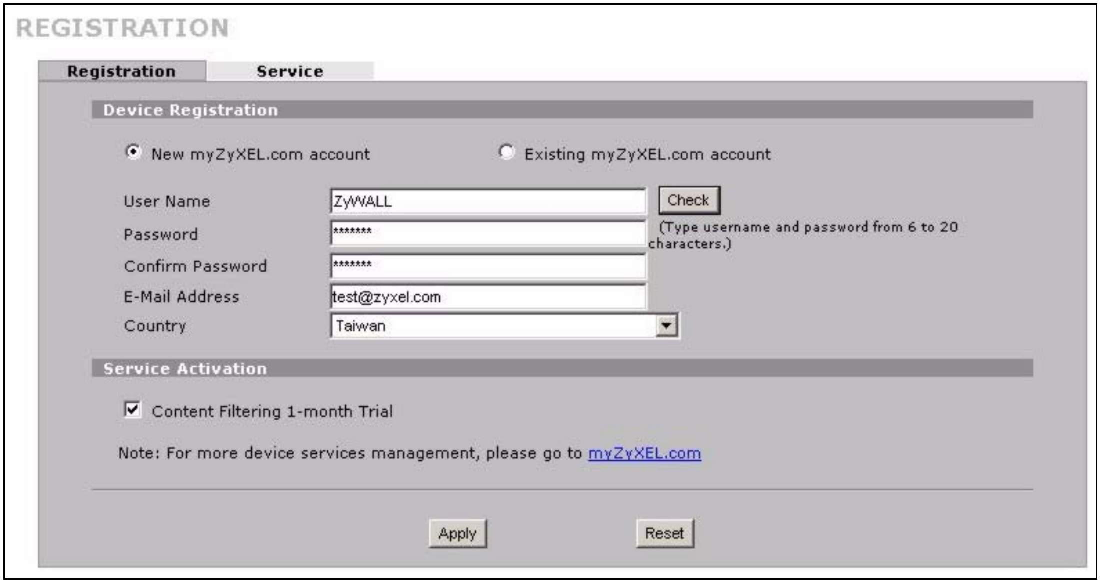
The ZyWALL can use the content filtering subscription service. Content filtering allows or blocks access to web sites. Subscribe to category-based content filtering to block access to categories of web sites based on content. Your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories. See the chapter about content filtering for more information.

✍ To use a subscription service, you have to register and activate the corresponding service at myZyXEL.com (through the ZyWALL).

## 5.2 Registration

Use this screen to register your ZyWALL with myZyXEL.com and activate the content filtering service. Click **REGISTRATION** in the navigation panel to open the screen as shown next.

**Figure 88** REGISTRATION



Device Registration

● New myZyXEL.com account ○ Existing myZyXEL.com account

User Name: ZyWALL

(Type username and password from 6 to 20 characters.)

Password: *******

Confirm Password: *******

E-Mail Address: test@zyxel.com

Country: Taiwan

Service Activation

☑ Content Filtering 1-month Trial

Note: For more device services management, please go to myZyXEL.com

The following table describes the labels in this screen.

**Table 20** REGISTRATION

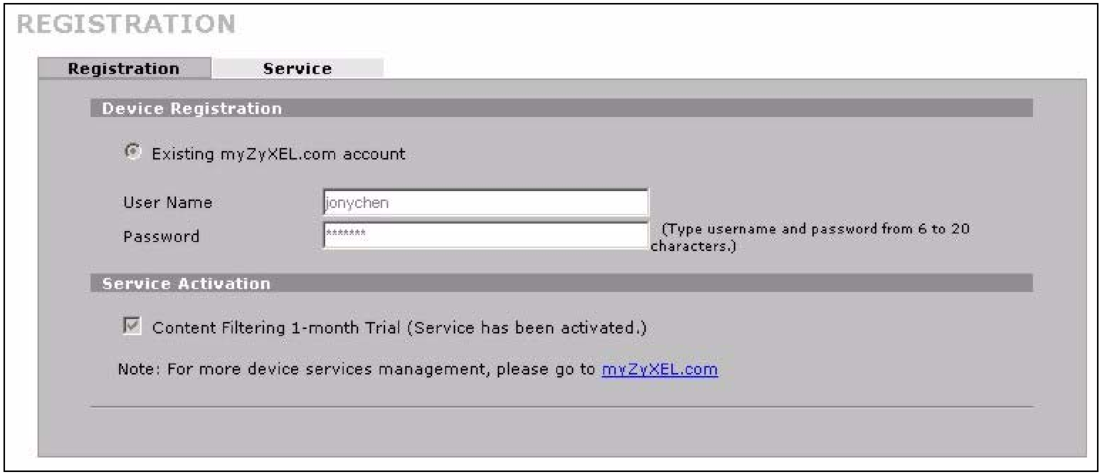
| LABEL | DESCRIPTION |
|---|---|
| Device Registration | If you select **Existing myZyXEL.com account**, only the **User Name** and **Password** fields are available. |
| New myZyXEL.com account | If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL. |
| Existing myZyXEL.com account | If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL. |
| User Name | Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Check | Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used. |
| Password | Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Confirm Password | Enter the password again for confirmation. |
| E-Mail Address | Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces. |
| Country | Select your country from the drop-down box list. |
| Service Activation | You can try trial service subscription. After the trial expires, you can buy an iCard and enter the license key in the **REGISTRATION > Service** screen to extend the service. |

**Table 20** REGISTRATION

| LABEL | DESCRIPTION |
|---|---|
| Content Filtering 1-month Trial | Select the check box to activate a trial. The trial period starts the day you activate the trial. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

If the ZyWALL is registered already, this screen is read-only and indicates whether trial services are activated. Use the **Service** screen to update your service subscription status.

**Figure 89** REGISTRATION: Registered Device



Device Registration

● Existing myZyXEL.com account

User Name: jonychen

Password: *******

(Type username and password from 6 to 20 characters.)

Service Activation

☑ Content Filtering 1-month Trial (Service has been activated.)

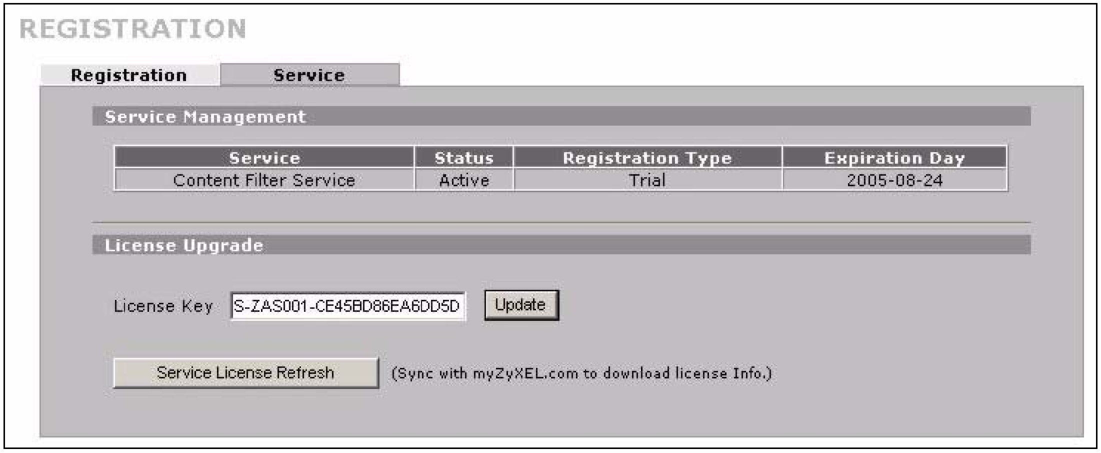
Note: For more device services management, please go to myZyXEL.com

## 5.3 Service

After you activate a trial, you can also use the **Service** screen to register and enter your iCard's PIN number (license key). Click **REGISTRATION** > **Service** to open the screen as shown next.

If you restore the ZyWALL to the default configuration file or upload a different configuration file after you register, click the **Service License Refresh** button to update license information.

**Figure 90** REGISTRATION > Service



| Service | Status | Registration Type | Expiration Day |
|---|---|---|---|
| Content Filter Service | Active | Trial | 2005-08-24 |

License Key: S-ZAS001-CE45BD86EA6DD5D

(Sync with myZyXEL.com to download license Info.)

The following table describes the labels in this screen.

**Table 21** REGISTRATION > Service

| LABEL | DESCRIPTION |
|---|---|
| Service Management | |
| Service | This field displays the service name available on the ZyWALL. |
| Status | This field displays whether a service is activated (**Active**) or not (**Inactive**). |
| Registration Type | This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard’s PIN number (**Standard**). |
| Expiration Day | This field displays the date your service expires. |
| License Upgrade | |
| License Key | Enter your iCard’s PIN number and click **Update** to activate or extend a standard service subscription.<br>If a standard service subscription runs out, you need to buy a new iCard (specific to your ZyWALL) and enter the new PIN number to extend the service. |
| Service License Refresh | Click this button to renew service license information (such as the license key, registration status and expiration day). |

# PART II

# Network

LAN Screens  (133)

Bridge Screens  (145)

WAN Screens  (151)

DMZ Screens  (171)

Wireless LAN  (181)

# 6

# LAN Screens

This chapter describes how to configure LAN settings. This chapter is only applicable when the ZyWALL is in router mode.

## 6.1 LAN, WAN and the ZyWALL

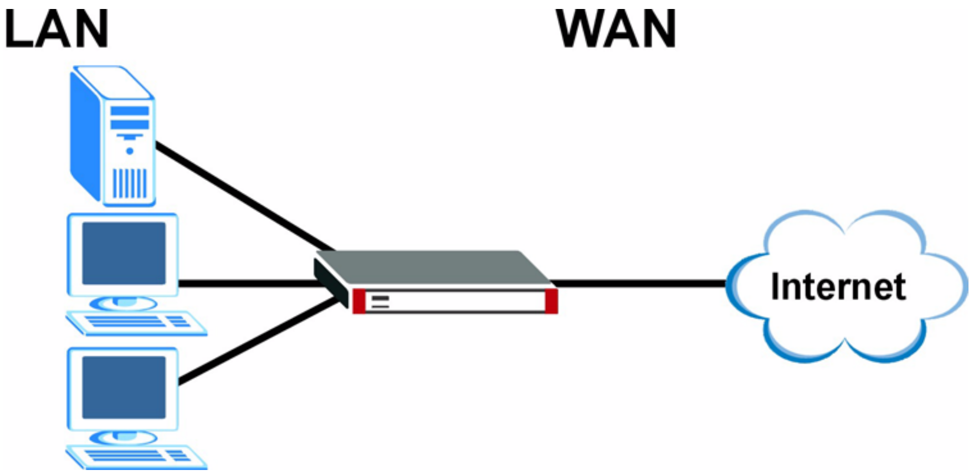
A network is a shared communication system to which many computers are attached.

The Local Area Network (LAN) includes the computers and networking devices in your home or office that you connect to the ZyWALL's LAN ports.

The Wide Area Network (WAN) is another network (most likely the Internet) that you connect to the ZyWALL's WAN port. See Chapter 8 on page 151 for how to use the WAN screens to set up your WAN connection.

The LAN and the WAN are two separate networks. The ZyWALL controls the traffic that goes between them. The following graphic gives an example.

**Figure 91** LAN and WAN



## 6.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyWALL. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. If you select 192.168.1.0 as the network number; it covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyWALL, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyWALL will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyWALL unless you are instructed to do otherwise.

## 6.2.1 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

## 6.3 DHCP

The ZyWALL can use DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) to automatically assign IP addresses subnet masks, gateways, and some network information like the IP addresses of DNS servers to the computers on your LAN. You can alternatively have the ZyWALL relay DHCP information from another DHCP server. If you disable the ZyWALL's DHCP service, you must have another DHCP server on your LAN, or else the computers must be manually configured.

### 6.3.1 IP Pool Setup

The ZyWALL is pre-configured with a pool of IP addresses for the computers on your LAN. See Chapter 46 on page 613 for the default IP pool range. Do not assign your LAN computers static IP addresses that are in the DHCP pool.

## 6.4 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

**RIP Version** controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

## 6.5 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address

224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyWALL queries all directly connected networks to gather group membership. After that, the ZyWALL periodically updates this information. IP multicasting can be enabled/ disabled on the ZyWALL LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

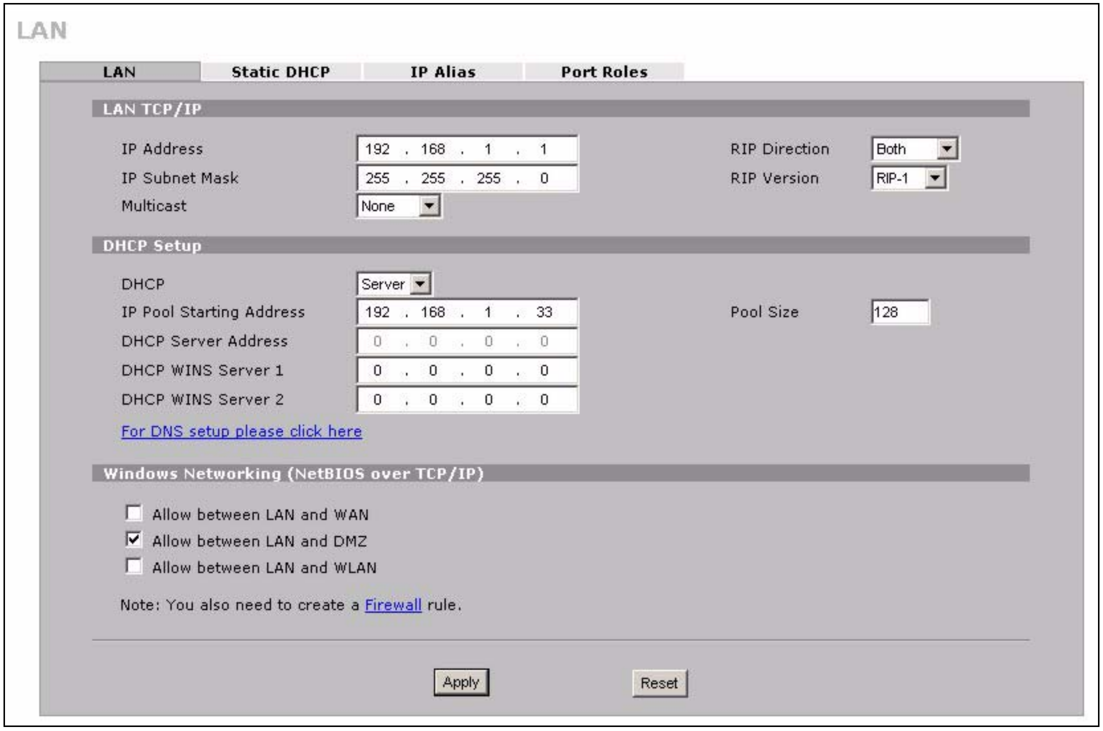
## 6.6 WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

## 6.7 LAN

Click **NETWORK** > **LAN** to open the **LAN** screen. Use this screen to configure the ZyWALL's IP address and other LAN TCP/IP settings as well as the built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

**Figure 92** NETWORK > LAN


LAN
LAN
Static DHCP
IP Alias
Port Roles
LAN TCP/IP
DHCP Setup
For DNS setup please click here
Windows Networking (NetBIOS over TCP/IP)
Apply
Reset

IP Address: 192 . 168 . 1 . 1
IP Subnet Mask: 255 . 255 . 255 . 0
Multicast: None
RIP Direction: Both
RIP Version: RIP-1

DHCP: Server
IP Pool Starting Address: 192 . 168 . 1 . 33
Pool Size: 128
DHCP Server Address: 0 . 0 . 0 . 0
DHCP WINS Server 1: 0 . 0 . 0 . 0
DHCP WINS Server 2: 0 . 0 . 0 . 0

☐ Allow between LAN and WAN
☑ Allow between LAN and DMZ
☐ Allow between LAN and WLAN

Note: You also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 22** NETWORK > LAN

| LABEL | DESCRIPTION |
|---|---|
| LAN TCP/IP | |
| IP Address | Type the IP address of your ZyWALL in dotted decimal notation. 192.168.1.1 is the factory default. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your ZyWALL automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |

**Table 22** NETWORK > LAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| Multicast | Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*. |
| DHCP Setup | |
| DHCP | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields.<br>Select **Relay** to have the ZyWALL forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field.<br>Select **None** to stop the ZyWALL from acting as a DHCP server. When you select **None**, you must have another DHCP server on your LAN, or else the computers must be manually configured. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| DHCP Server Address | Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| DHCP WINS Server 1, 2 | Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. |
| Windows Networking (NetBIOS over TCP/IP) | NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN. |
| Allow between LAN and WAN | Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. |
| Allow between LAN and DMZ | Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to enable the default DMZ to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN. |
| Allow between LAN and WLAN | Select this check box to forward NetBIOS packets from the LAN to the WLAN and from the WLAN to the LAN.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WLAN and from the WLAN to the LAN. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

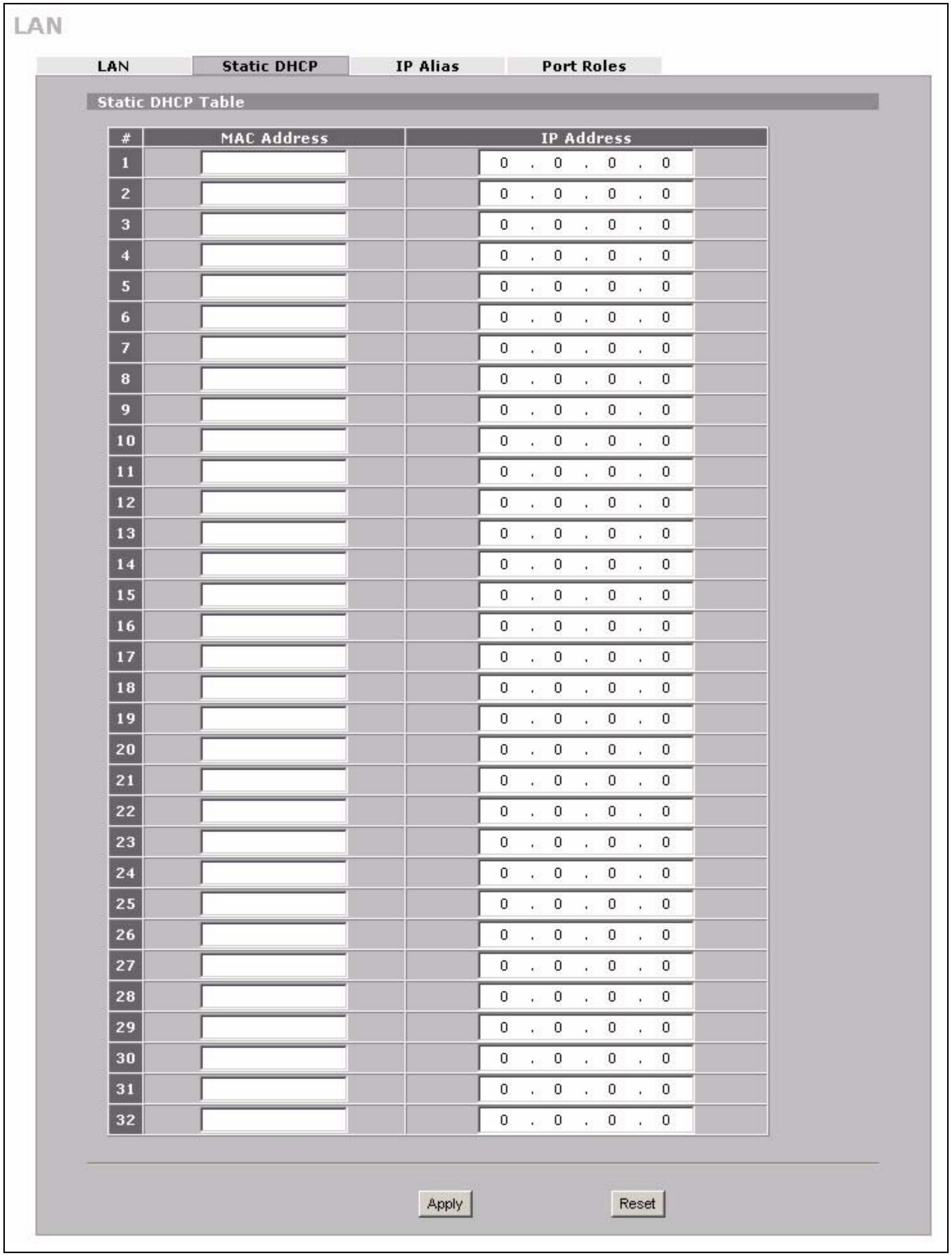
## 6.8 LAN Static DHCP

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your ZyWALL's static DHCP settings, click **NETWORK** > **LAN** > **Static DHCP**. The screen appears as shown.

**Figure 93** NETWORK > LAN > Static DHCP



| # | MAC Address | IP Address |
|---|---|---|
| 1 | | 0 . 0 . 0 . 0 |
| 2 | | 0 . 0 . 0 . 0 |
| 3 | | 0 . 0 . 0 . 0 |
| 4 | | 0 . 0 . 0 . 0 |
| 5 | | 0 . 0 . 0 . 0 |
| 6 | | 0 . 0 . 0 . 0 |
| 7 | | 0 . 0 . 0 . 0 |
| 8 | | 0 . 0 . 0 . 0 |
| 9 | | 0 . 0 . 0 . 0 |
| 10 | | 0 . 0 . 0 . 0 |
| 11 | | 0 . 0 . 0 . 0 |
| 12 | | 0 . 0 . 0 . 0 |
| 13 | | 0 . 0 . 0 . 0 |
| 14 | | 0 . 0 . 0 . 0 |
| 15 | | 0 . 0 . 0 . 0 |
| 16 | | 0 . 0 . 0 . 0 |
| 17 | | 0 . 0 . 0 . 0 |
| 18 | | 0 . 0 . 0 . 0 |
| 19 | | 0 . 0 . 0 . 0 |
| 20 | | 0 . 0 . 0 . 0 |
| 21 | | 0 . 0 . 0 . 0 |
| 22 | | 0 . 0 . 0 . 0 |
| 23 | | 0 . 0 . 0 . 0 |
| 24 | | 0 . 0 . 0 . 0 |
| 25 | | 0 . 0 . 0 . 0 |
| 26 | | 0 . 0 . 0 . 0 |
| 27 | | 0 . 0 . 0 . 0 |
| 28 | | 0 . 0 . 0 . 0 |
| 29 | | 0 . 0 . 0 . 0 |
| 30 | | 0 . 0 . 0 . 0 |
| 31 | | 0 . 0 . 0 . 0 |
| 32 | | 0 . 0 . 0 . 0 |

The following table describes the labels in this screen.

**Table 23** NETWORK > LAN > Static DHCP

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the Static IP table entry (row). |
| MAC Address | Type the MAC address of a computer on your LAN. |
| IP Address | Type the IP address that you want to assign to the computer on your LAN.<br>Alternatively, click the right mouse button to copy and/or paste the IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 6.9 LAN IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

The ZyWALL has a single LAN interface. Even though more than one of ports 1~4 may be in the LAN port role, they are all still part of a single physical Ethernet interface and all use the same IP address.

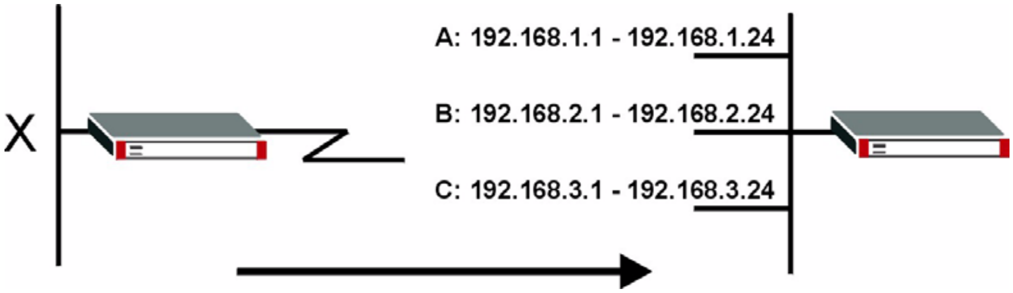
The ZyWALL supports three logical LAN interfaces via its single physical LAN Ethernet interface. The ZyWALL itself is the gateway for each of the logical LAN networks.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Make sure that the subnets of the logical networks do not overlap.

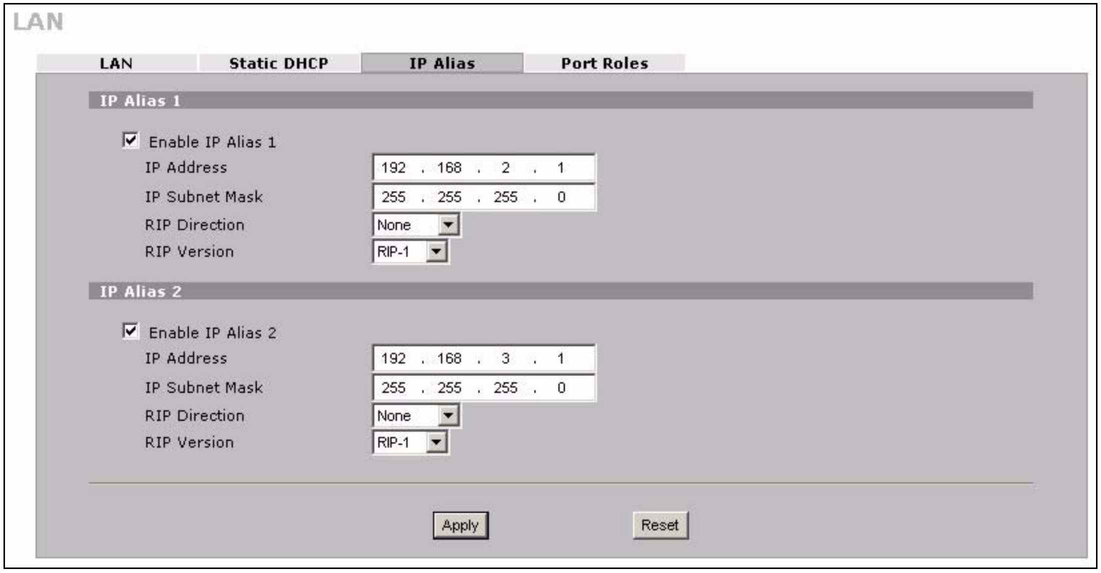
The following figure shows a LAN divided into subnets A, B, and C.

**Figure 94** Physical Network & Partitioned Logical Networks


X
A: 192.168.1.1 - 192.168.1.24
B: 192.168.2.1 - 192.168.2.24
C: 192.168.3.1 - 192.168.3.24

To change your ZyWALL’s IP alias settings, click **NETWORK** > **LAN** > **IP Alias**. The screen appears as shown.

**Figure 95** NETWORK > LAN > IP Alias



IP Alias 1

☑ Enable IP Alias 1
IP Address 192 . 168 . 2 . 1
IP Subnet Mask 255 . 255 . 255 . 0
RIP Direction None
RIP Version RIP-1

IP Alias 2

☑ Enable IP Alias 2
IP Address 192 . 168 . 3 . 1
IP Subnet Mask 255 . 255 . 255 . 0
RIP Direction None
RIP Version RIP-1

The following table describes the labels in this screen.

**Table 24** NETWORK > LAN > IP Alias

| LABEL | DESCRIPTION |
|---|---|
| Enable IP Alias 1, 2 | Select the check box to configure another LAN network for the ZyWALL. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation.<br>Alternatively, click the right mouse button to copy and/or paste the IP address. |
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 6.10 LAN Port Roles

Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Ports 1~4 on the ZyWALL can be part of the LAN, DMZ or WLAN interface.

Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

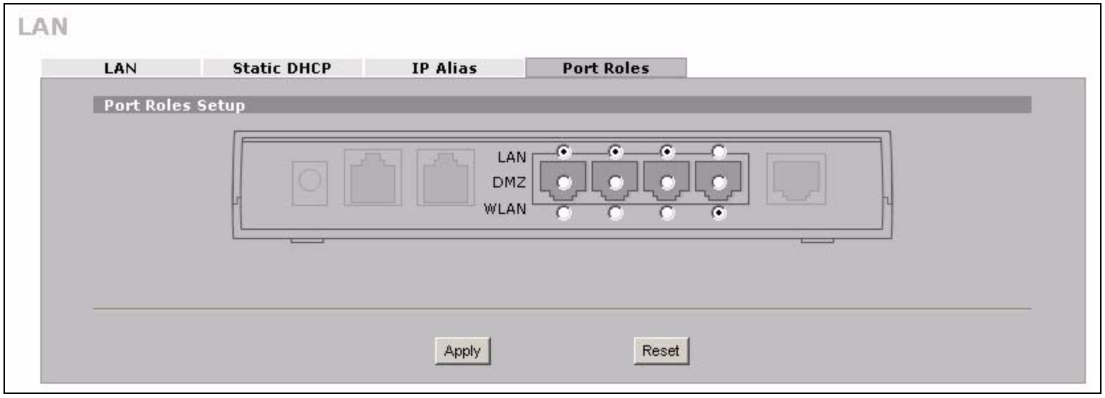
1 A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyWALL's LAN, DMZ or WLAN IP address.
2 Use the appropriate LAN, DMZ or WLAN IP address to access the ZyWALL.

To change your ZyWALL's port role settings, click **NETWORK** > **LAN** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. On the ZyWALL, ports 1 to 4 are all LAN ports by default.

Your changes are also reflected in the **DMZ Port Roles** and **WLAN Port Roles** screens.

**Figure 96** NETWORK > LAN > Port Roles



The following table describes the labels in this screen.

**Table 25** NETWORK > LAN > Port Roles

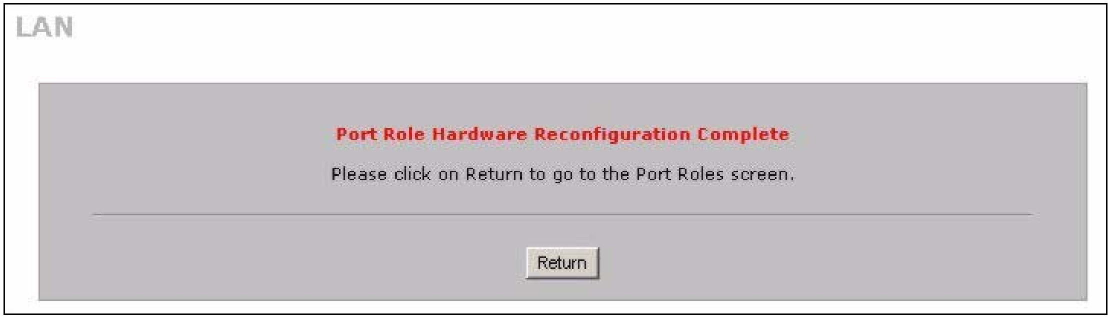
| LABEL | DESCRIPTION |
|---|---|
| LAN | Select a port's LAN radio button to use the port as part of the LAN. The port will use the ZyWALL's LAN IP address and MAC address. |
| DMZ | Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the ZyWALL's DMZ IP address and MAC address. |
| WLAN | Select a port's WLAN radio button to use the port as part of the WLAN.<br>The port will use the ZyWALL's WLAN IP address and MAC address. |

**Table 25** NETWORK > LAN > Port Roles (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

After you change the LAN/DMZ/WLAN port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

**Figure 97** Port Roles Change Complete



Port Role Hardware Reconfiguration Complete

Please click on Return to go to the Port Roles screen.

# 7

# Bridge Screens

This chapter describes how to configure bridge settings. This chapter is only applicable when the ZyWALL is in bridge mode.

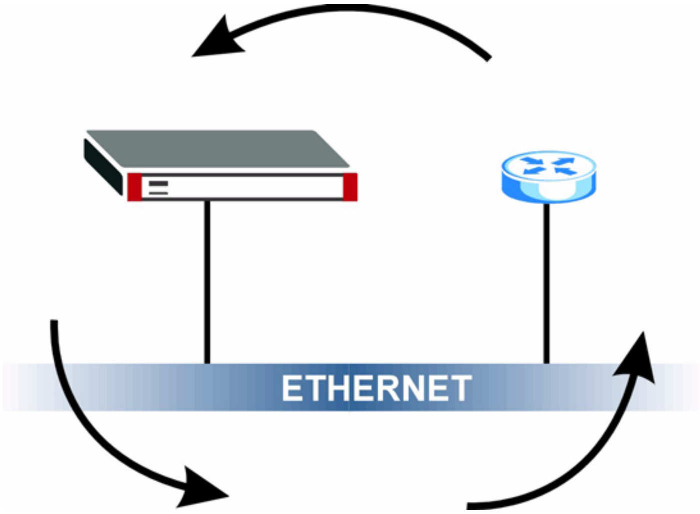
## 7.1 Bridge Loop

The ZyWALL can act as a bridge between a switch and a wired LAN or between two routers.

Be careful to avoid bridge loops when you enable bridging in the ZyWALL. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following example shows the network topology that can lead to this problem:

- If your ZyWALL (in bridge mode) is connected to a wired LAN while communicating with another bridge or a switch that is also connected to the same wired LAN as shown next.

**Figure 98** Bridge Loop: Bridge Connected to Wired LAN



To prevent bridge loops, ensure that your ZyWALL is not set to bridge mode while connected to two wired segments of the same LAN or you enable RSTP in the **Bridge** screen.

## 7.2 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

### 7.2.1 Rapid STP

The ZyWALL uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP, topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

### 7.2.2 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame from the root bridge to that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

**Table 26** STP Path Costs

| | LINK SPEED | RECOMMENDED VALUE | RECOMMENDED RANGE | ALLOWED RANGE |
|---|---|---|---|---|
| Path Cost | 4Mbps | 250 | 100 to 1000 | 1 to 65535 |
| Path Cost | 10Mbps | 100 | 50 to 600 | 1 to 65535 |
| Path Cost | 16Mbps | 62 | 40 to 400 | 1 to 65535 |
| Path Cost | 100Mbps | 19 | 10 to 60 | 1 to 65535 |
| Path Cost | 1Gbps | 4 | 3 to 10 | 1 to 65535 |
| Path Cost | 10Gbps | 2 | 1 to 5 | 1 to 65535 |

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

### 7.2.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

### 7.2.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

**Table 27** STP Port States

| PORT STATE | DESCRIPTION |
|---|---|
| Disabled | STP is disabled (default). |
| Blocking | Only configuration and management BPDUs are received and processed. |
| Listening | All BPDUs are received and processed. |
| Learning | All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded. |
| Forwarding | All BPDUs are received and processed. All information frames are received and forwarded. |

## 7.3 Bridge

Select **Bridge** and click **Apply** in the **MAINTENANCE Device Mode** screen to have the ZyWALL function as a bridge.

In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.

You can use the firewall and VPN in bridge mode. See the user’s guide for a list of other features that are available in bridge mode.

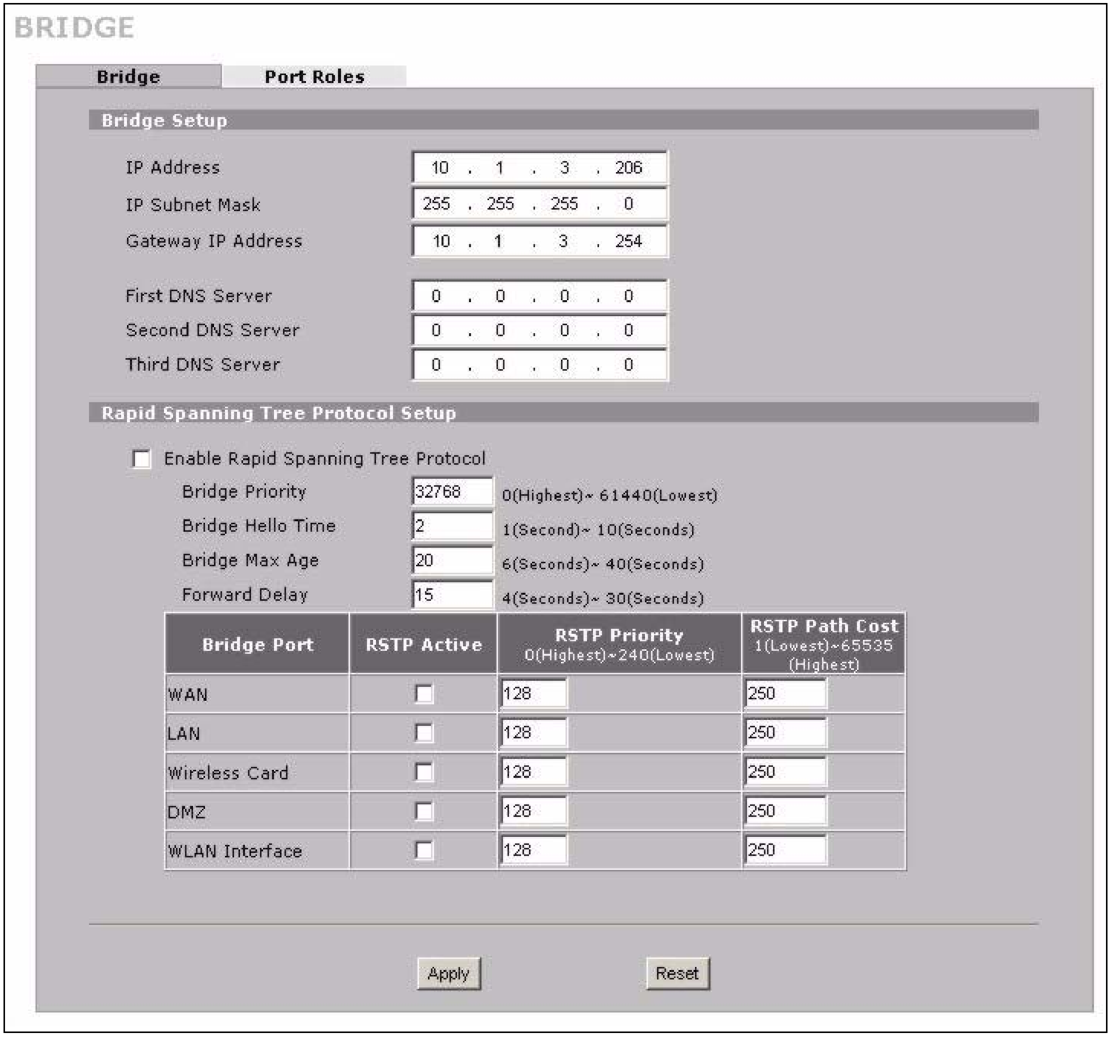
Click **NETWORK** > **BRIDGE** to display the screen shown next. Use this screen to configure bridge and RSTP (Rapid Spanning Tree Protocol) settings.

---

In bridge mode, if you need to let DHCP clients behind the ZyWALL use a DHCP server on the WAN, enable the default WAN to LAN firewall rule for the **BOOTP_CLIENT** service.

---

**Figure 99** NETWORK > Bridge



| | |
|---|---|
| IP Address | 10 . 1 . 3 . 206 |
| IP Subnet Mask | 255 . 255 . 255 . 0 |
| Gateway IP Address | 10 . 1 . 3 . 254 |
| First DNS Server | 0 . 0 . 0 . 0 |
| Second DNS Server | 0 . 0 . 0 . 0 |
| Third DNS Server | 0 . 0 . 0 . 0 |

☐ Enable Rapid Spanning Tree Protocol

| | | |
|---|---|---|
| Bridge Priority | 32768 | 0(Highest)~ 61440(Lowest) |
| Bridge Hello Time | 2 | 1(Second)~ 10(Seconds) |
| Bridge Max Age | 20 | 6(Seconds)~ 40(Seconds) |
| Forward Delay | 15 | 4(Seconds)~ 30(Seconds) |

| Bridge Port | RSTP Active | RSTP Priority 0(Highest)~240(Lowest) | RSTP Path Cost 1(Lowest)~65535 (Highest) |
|---|---|---|---|
| WAN | ☐ | 128 | 250 |
| LAN | ☐ | 128 | 250 |
| Wireless Card | ☐ | 128 | 250 |
| DMZ | ☐ | 128 | 250 |
| WLAN Interface | ☐ | 128 | 250 |

The following table describes the labels in this screen.

**Table 28** NETWORK > Bridge

| LABEL | DESCRIPTION |
|---|---|
| Bridge IP Address Setup | |
| IP Address | Type the IP address of your ZyWALL in dotted decimal notation. Use an IP address in the same subnet as the network to which you connect the ZyWALL. Make sure the IP address does not conflict with any other device on the network. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. |
| Gateway IP Address | Enter the gateway IP address. |
| First/Second/Third DNS Server | DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for content filtering, the time server, etc.<br>If you have the IP address(es) of the DNS server(s), enter the DNS server's IP address(es) in the field(s) to the right. |

**Table 28** NETWORK > Bridge (continued)

| LABEL | DESCRIPTION |
|---|---|
| Rapid Spanning Tree Protocol Setup | |
| Enable Rapid Spanning Tree Protocol | Select the check box to activate RSTP on the ZyWALL. |
| Bridge Priority | Enter a number between 0 and 61440 as bridge priority of the ZyWALL.<br>Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the root. If multiple devices have the lowest priority, the device with the lowest MAC address becomes the root.<br>The lower the numeric value you assign, the higher the priority for this bridge.<br>Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forward Delay. |
| Bridge Hello Time | Enter an interval (between 1 and 10) in seconds that the root bridge waits before sending a hello packet. |
| Bridge Max Age | Enter an interval (between 6 and 40) in seconds that a bridge waits to get a Hello BPDU from the root bridge. |
| Forward Delay | Enter the length of time (between 4 and 30) in seconds that a bridge remains in the listening and learning port states. The default is 15 seconds. |
| Bridge Port | This is the bridge port type. |
| RSTP Active | Select the check box to enable RSTP on the corresponding port. |
| RSTP Priority 0(Highest)~240(Lowest) | Enter a number between 0 and 240 as RSTP priority for the corresponding port. 0 is the highest. |
| RSTP Path Cost 1(Lowest)~65535(Highest) | Enter a number between 1 and 65535 as RSTP path cost for the corresponding port. 65535 is the highest. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 7.4 Bridge Port Roles

Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Ports 1~4 on the ZyWALL can be part of the LAN, DMZ or WLAN interface.

To change your ZyWALL’s port role settings, click **NETWORK** > **BRIDGE** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. On the ZyWALL, ports 1 to 4 are all LAN ports by default.

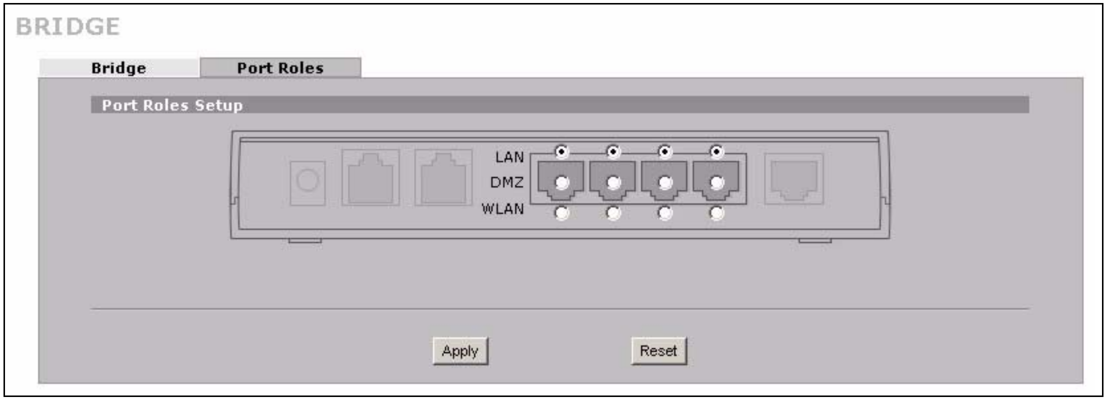


**Figure 100** NETWORK > Bridge > Port Roles

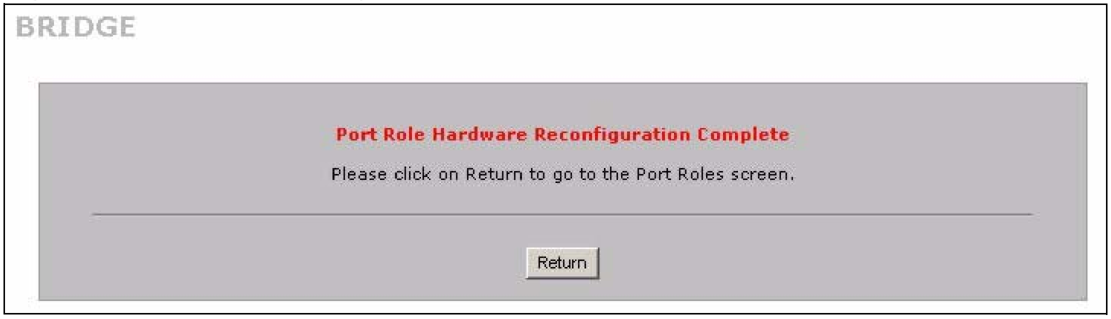
The following table describes the labels in this screen.

**Table 29** NETWORK > Bridge > Port Roles

| LABEL | DESCRIPTION |
|---|---|
| LAN | Select a port's LAN radio button to use the port as part of the LAN. |
| DMZ | Select a port's DMZ radio button to use the port as part of the DMZ. |
| WLAN | Select a port's WLAN radio button to use the port as part of the WLAN. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

After you change the LAN/DMZ/WLAN port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

**Figure 101** Port Roles Change Complete



Port Role Hardware Reconfiguration Complete

Please click on Return to go to the Port Roles screen.

# 8

# WAN Screens

This chapter describes how to configure WAN settings.

## 8.1 WAN Overview

- Use the **Route** screen to configure route priority for the ZyWALL.
- Use the **WAN** screen to configure the WAN port for Internet access on the ZyWALL.
- Use the **Traffic Redirect** screen to configure an alternative gateway.
- Use the **Dial Backup** screen to configure the backup WAN dial-up connection.

## 8.2 TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

1. The metric sets the priority for the ZyWALL's routes to the Internet. Each route must have a unique metric.
2. The priorities of the WAN port routes must always be higher than the dial-backup and traffic redirect route priorities.

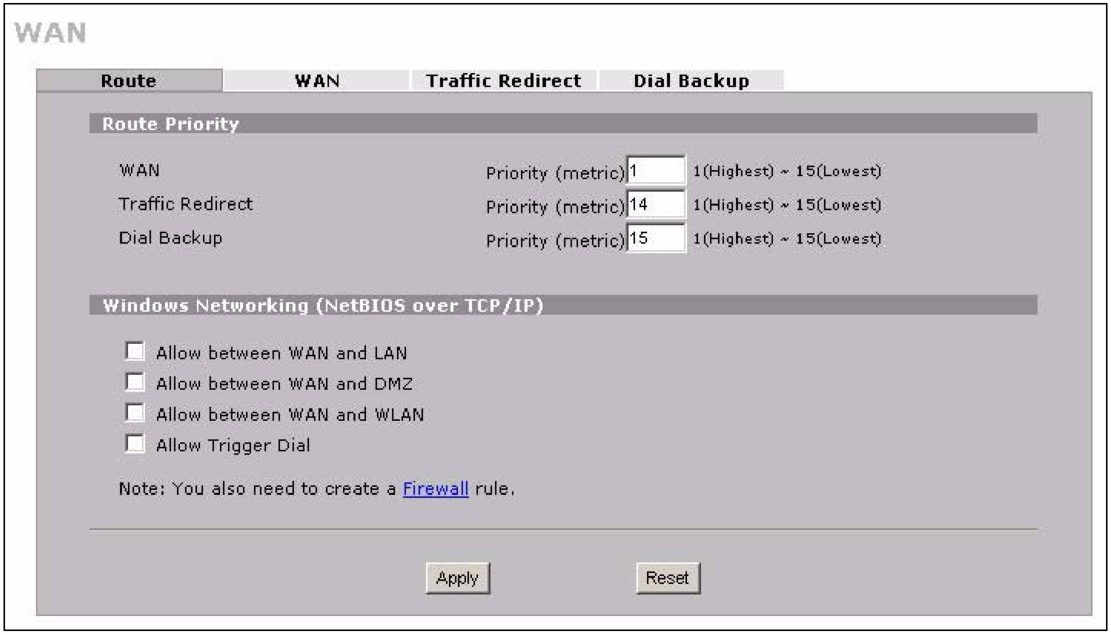
If the WAN port route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the WAN port route acts as the primary default route. If the WAN port route fails to connect to the Internet, the ZyWALL tries the traffic-redirect route next. In the same manner, the ZyWALL uses the dial-backup route if the traffic-redirect route also fails.

The dial-backup or traffic redirect routes cannot take priority over the WAN routes.

## 8.3 WAN Route

Click **NETWORK** > **WAN** to open the **Route** screen. Use this screen to configure the priorities of the ZyWALL’s routes and settings for Windows Networking traffic.

**Figure 102** NETWORK > WAN Route



Route Priority

WAN Priority (metric) 1 1(Highest) ~ 15(Lowest)
Traffic Redirect Priority (metric) 14 1(Highest) ~ 15(Lowest)
Dial Backup Priority (metric) 15 1(Highest) ~ 15(Lowest)

Windows Networking (NetBIOS over TCP/IP)

☐ Allow between WAN and LAN
☐ Allow between WAN and DMZ
☐ Allow between WAN and WLAN
☐ Allow Trigger Dial

Note: You also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 30** NETWORK > WAN Route

| LABEL | DESCRIPTION |
|---|---|
| Route Priority | |
| WAN<br>Traffic Redirect<br>Dial Backup | The default WAN connection is "1' as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is **WAN**, **Traffic Redirect** and then **Dial Backup**:<br>You have two choices for an auxiliary connection (**Traffic Redirect** and **Dial Backup**) in the event that your regular WAN connection goes down. If **Dial Backup** is preferred to **Traffic Redirect**, then type "14" in the **Dial Backup Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of "15").<br>The **Dial Backup** field is available only when you enable the corresponding dial backup feature in the **Dial Backup** screen. |
| Windows Networking (NetBIOS over TCP/IP): | NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. |
| Allow between WAN and LAN | Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. |
| Allow between WAN and DMZ | Select this check box to forward NetBIOS packets from the WAN to the DMZ and from the DMZ to the WAN.<br>Clear this check box to block all NetBIOS packets going from the WAN to the DMZ and from the DMZ to the WAN. |
| Allow between WAN and WLAN | Select this check box to forward NetBIOS packets from the WLAN to the WAN and from the WAN to the WLAN.<br>Clear this check box to block all NetBIOS packets going from the WLAN to the WAN and from the WAN to the WLAN. |

**Table 30** NETWORK > WAN Route (continued)

| LABEL | DESCRIPTION |
|---|---|
| Allow Trigger Dial | Select this option to allow NetBIOS packets to initiate calls. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.4 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

**Table 31** Private IP Address Ranges

| | | |
|---|---|---|
| 10.0.0.0 | - | 10.255.255.255 |
| 172.16.0.0 | - | 172.31.255.255 |
| 192.168.0.0 | - | 192.168.255.255 |

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

## 8.5 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyWALL can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

3 You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Section 20.5.1 on page 366).

## 8.6 WAN MAC Address

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

## 8.7 WAN

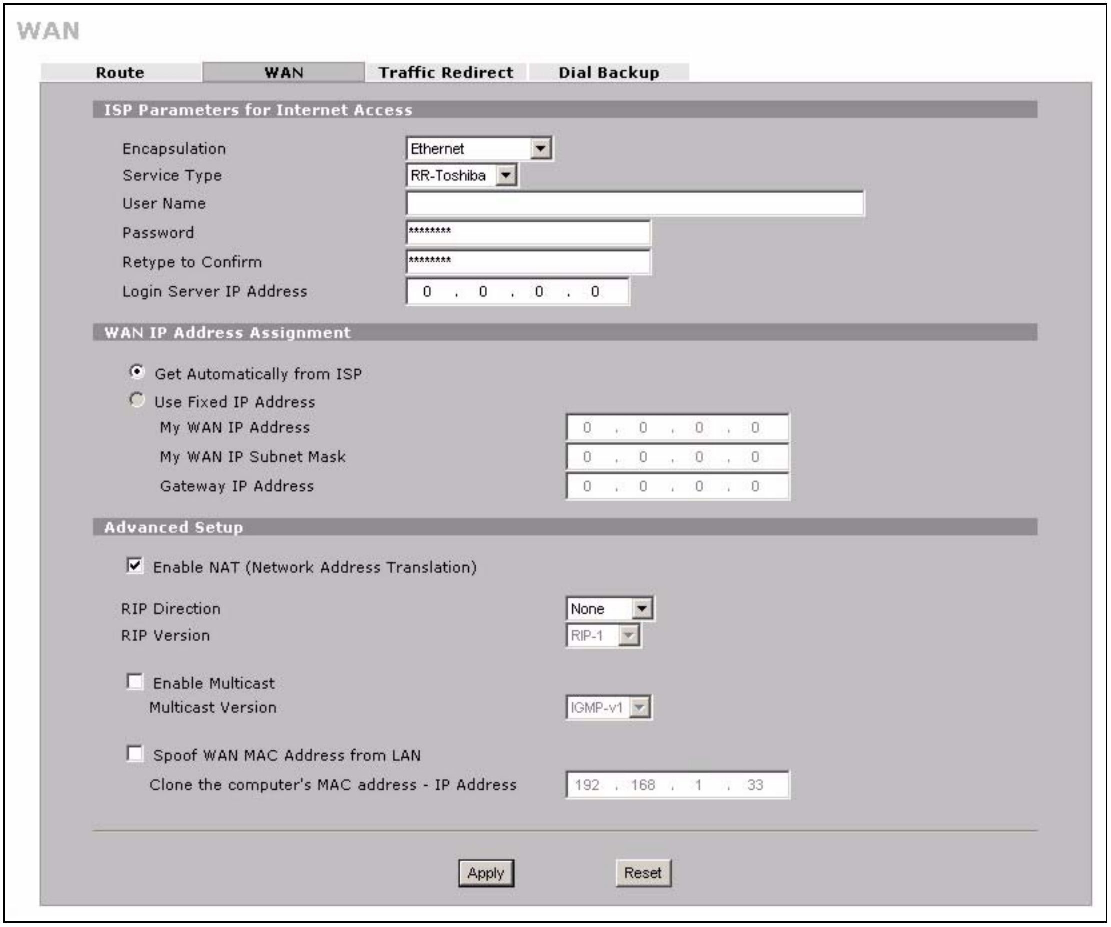
To change your ZyWALL's WAN ISP, IP and MAC settings, click **NETWORK** > **WAN** > **WAN**. The screen differs by the encapsulation.

### 8.7.1 WAN Ethernet Encapsulation

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/ZyWALL** firewall rule for those packets. Contact your ISP to find the correct port number.

The screen shown next is for **Ethernet** encapsulation.

**Figure 103** NETWORK > WAN > WAN (Ethernet Encapsulation)



ISP Parameters for Internet Access

Encapsulation: Ethernet
Service Type: RR-Toshiba
User Name:
Password: ********
Retype to Confirm: ********
Login Server IP Address: 0 . 0 . 0 . 0

WAN IP Address Assignment

● Get Automatically from ISP
○ Use Fixed IP Address
My WAN IP Address: 0 . 0 . 0 . 0
My WAN IP Subnet Mask: 0 . 0 . 0 . 0
Gateway IP Address: 0 . 0 . 0 . 0

Advanced Setup

☑ Enable NAT (Network Address Translation)
RIP Direction: None
RIP Version: RIP-1
☐ Enable Multicast
Multicast Version: IGMP-v1
☐ Spoof WAN MAC Address from LAN
Clone the computer's MAC address - IP Address: 192 . 168 . 1 . 33

The following table describes the labels in this screen.

**Table 32** NETWORK > WAN > WAN (Ethernet Encapsulation)

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | You must choose the Ethernet option when the WAN port is used as a regular Ethernet. |
| Service Type | Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**.<br>The following fields do not appear with the **Standard** service type. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to Confirm | Type your password again to make sure that you have entered is correctly. |
| Login Server IP Address | Type the authentication server IP address here if your ISP gave you one.<br>This field is not available for Telia Login. |
| Login Server (Telia Login only) | Type the domain name of the Telia login server, for example login1.telia.com. |

**Table 32** NETWORK > WAN > WAN (Ethernet Encapsulation) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Relogin Every(min) (Telia Login only) | The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyWALL to wait between logins. |
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use Fixed IP Address | Select this option If the ISP assigned a fixed IP address. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address**. |
| My WAN IP Subnet Mask | Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. |
| Gateway IP Address | Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. |
| Advanced Setup | |
| Enable NAT (Network Address Translation) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Select this check box to enable NAT. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives.<br>When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |

**Table 32** NETWORK > WAN > WAN (Ethernet Encapsulation) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Multicast Version | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Spoof WAN MAC Address | You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN.<br>Otherwise, select the check box next to **Spoof WAN MAC Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. |
| Clone the computer's MAC address – IP Address | Enter the IP address of the computer on the LAN whose MAC you are cloning.<br>It is recommended that you clone the MAC address prior to hooking up the WAN port. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.7.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

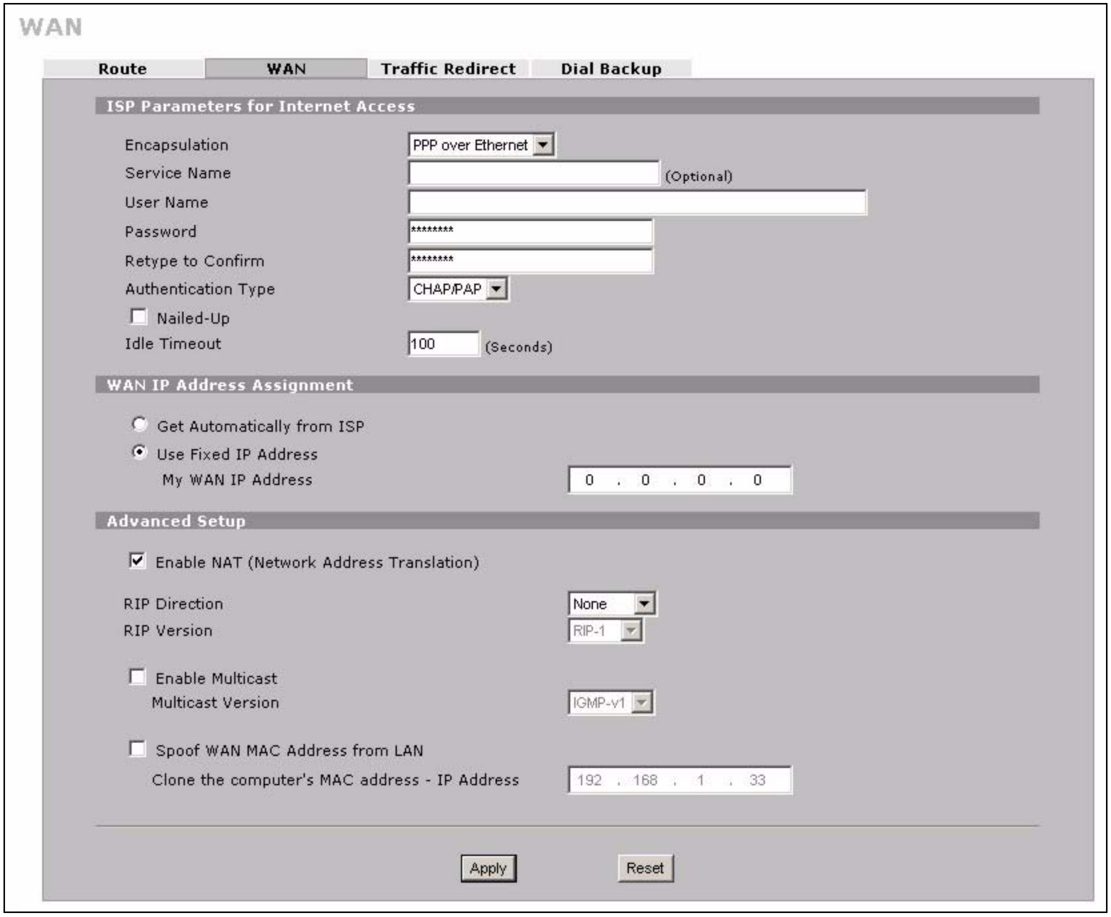
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyWALL (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyWALL does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

**Figure 104** NETWORK > WAN > WAN (PPPoE Encapsulation)



ISP Parameters for Internet Access

Encapsulation: PPP over Ethernet
Service Name: (Optional)
User Name:
Password: ********
Retype to Confirm: ********
Authentication Type: CHAP/PAP
☐ Nailed-Up
Idle Timeout: 100 (Seconds)

WAN IP Address Assignment

○ Get Automatically from ISP
● Use Fixed IP Address
My WAN IP Address: 0 . 0 . 0 . 0

Advanced Setup

☑ Enable NAT (Network Address Translation)

RIP Direction: None
RIP Version: RIP-1

☐ Enable Multicast
Multicast Version: IGMP-v1

☐ Spoof WAN MAC Address from LAN
Clone the computer's MAC address - IP Address: 192 . 168 . 1 . 33

The following table describes the labels in this screen.

**Table 33** NETWORK > WAN > WAN (PPPoE Encapsulation)

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. DSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access. |
| Service Name | Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server. This field is optional. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to Confirm | Type your password again to make sure that you have entered is correctly. |

**Table 33** NETWORK > WAN > WAN (PPPoE Encapsulation) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your ZyWALL accepts CHAP only.<br>**PAP** - Your ZyWALL accepts PAP only. |
| Nailed-Up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server. |
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use Fixed IP Address | Select this option If the ISP assigned a fixed IP address. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address.** |
| Advanced Setup | |
| Enable NAT (Network Address Translation) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Select this checkbox to enable NAT.<br>For more information about NAT see Chapter 17 on page 331. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives.<br>When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |

**Table 33** NETWORK > WAN > WAN (PPPoE Encapsulation) (continued)

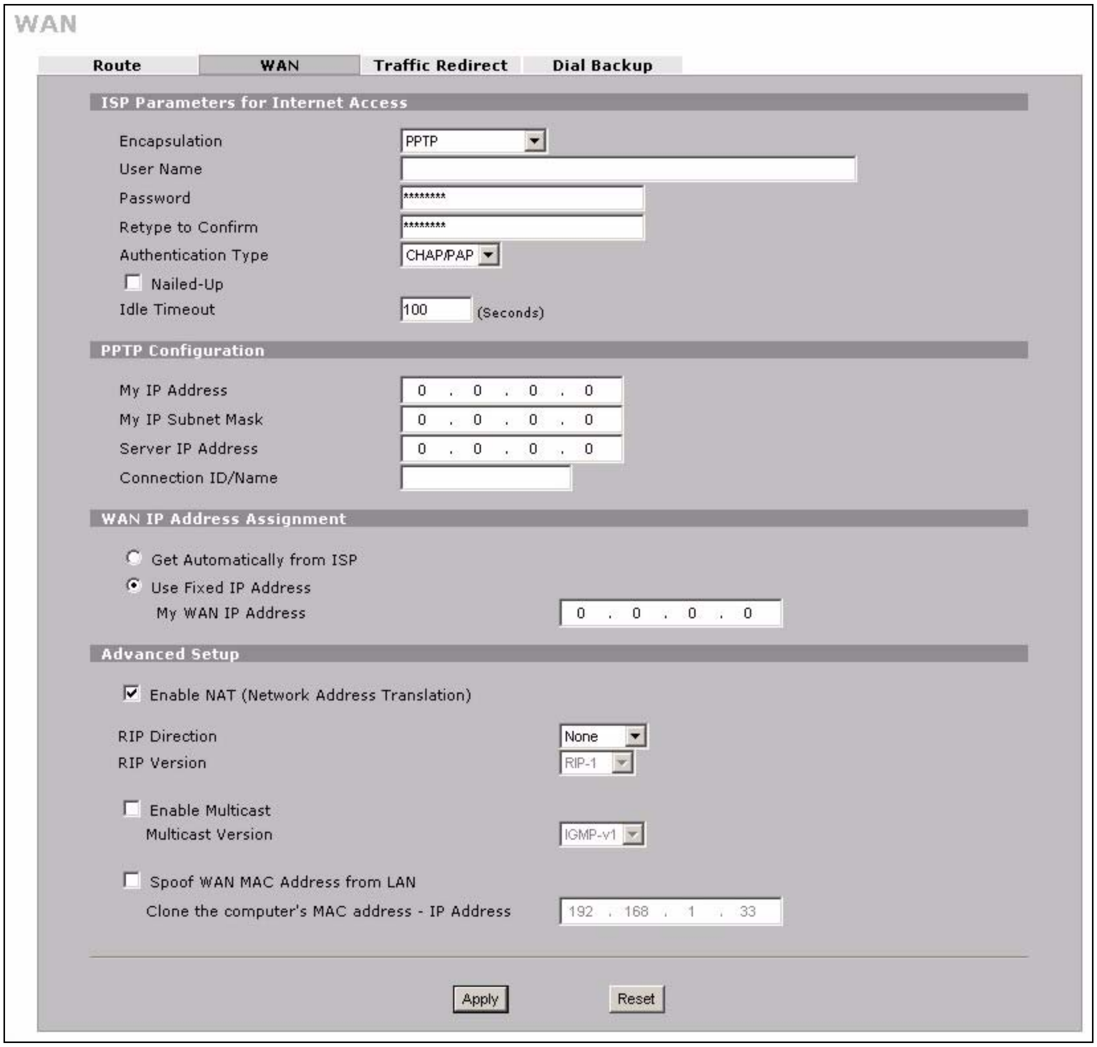
| LABEL | DESCRIPTION |
|---|---|
| Multicast Version | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Spoof WAN MAC Address | You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN.<br>Otherwise, select the check box next to **Spoof WAN MAC Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. |
| Clone the computer's MAC address – IP Address | Enter the IP address of the computer on the LAN whose MAC you are cloning.<br>It is recommended that you clone the MAC address prior to hooking up the WAN port. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

### 8.7.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The screen shown next is for **PPTP** encapsulation.

**Figure 105** NETWORK > WAN > WAN (PPTP Encapsulation)



Encapsulation: PPTP
User Name:
Password: ********
Retype to Confirm: ********
Authentication Type: CHAP/PAP
☐ Nailed-Up
Idle Timeout: 100 (Seconds)

My IP Address: 0 . 0 . 0 . 0
My IP Subnet Mask: 0 . 0 . 0 . 0
Server IP Address: 0 . 0 . 0 . 0
Connection ID/Name:

○ Get Automatically from ISP
● Use Fixed IP Address
My WAN IP Address: 0 . 0 . 0 . 0

☑ Enable NAT (Network Address Translation)
RIP Direction: None
RIP Version: RIP-1
☐ Enable Multicast
Multicast Version: IGMP-v1
☐ Spoof WAN MAC Address from LAN
Clone the computer's MAC address - IP Address: 192 . 168 . 1 . 33

The following table describes the labels in this screen.

**Table 34** NETWORK > WAN > WAN (PPTP Encapsulation)

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The ZyWALL supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to Confirm | Type your password again to make sure that you have entered is correctly. |

**Table 34** NETWORK > WAN > WAN (PPTP Encapsulation) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your ZyWALL accepts CHAP only.<br>**PAP** - Your ZyWALL accepts PAP only. |
| Nailed-up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPTP server. |
| PPTP Configuration | |
| My IP Address | Type the (static) IP address assigned to you by your ISP. |
| My IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| Server IP Address | Type the IP address of the PPTP server. |
| Connection ID/ Name | Type your identification name for the PPTP server. |
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use Fixed IP Address | Select this option If the ISP assigned a fixed IP address. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address**. |
| Advanced Setup | |
| Enable NAT (Network Address Translation) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Select this checkbox to enable NAT.<br>For more information about NAT see Chapter 17 on page 331. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives.<br>When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |

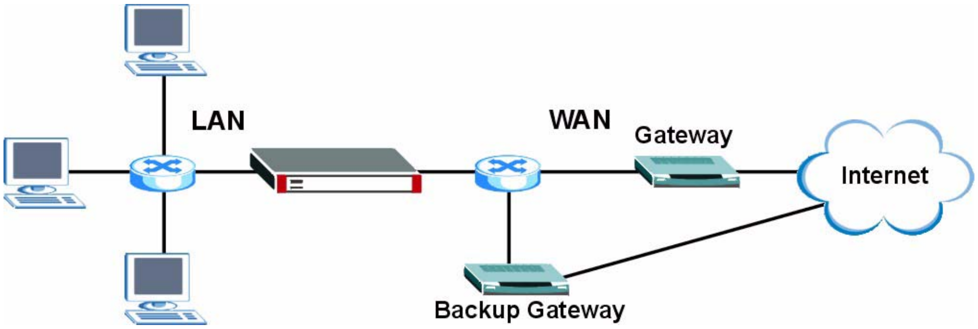
**Table 34** NETWORK > WAN > WAN (PPTP Encapsulation) (continued)

| LABEL | DESCRIPTION |
|---|---|
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |
| Multicast Version | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Spoof WAN MAC Address | You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN.<br>Otherwise, select the check box next to **Spoof WAN MAC Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. |
| Clone the computer's MAC address – IP Address | Enter the IP address of the computer on the LAN whose MAC you are cloning.<br>It is recommended that you clone the MAC address prior to hooking up the WAN port. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.8 Traffic Redirect

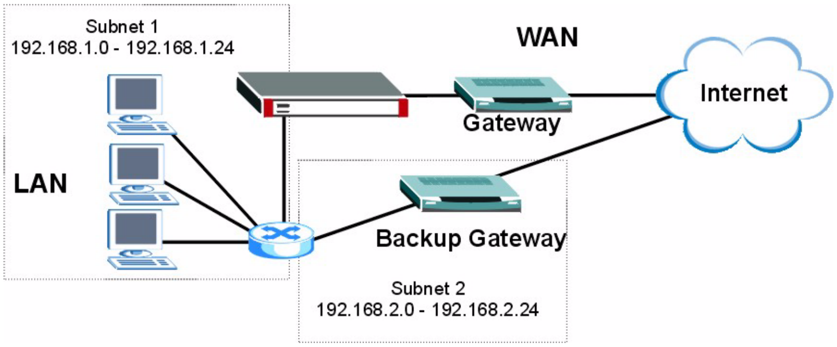
Traffic redirect forwards WAN traffic to a backup gateway when the ZyWALL cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyWALL still provides firewall protection for the LAN.

**Figure 106** Traffic Redirect WAN Setup


LAN
WAN
Gateway
Internet
Backup Gateway

IP alias allows you to avoid triangle route security issues when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the ZyWALL itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/ZyWALL firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

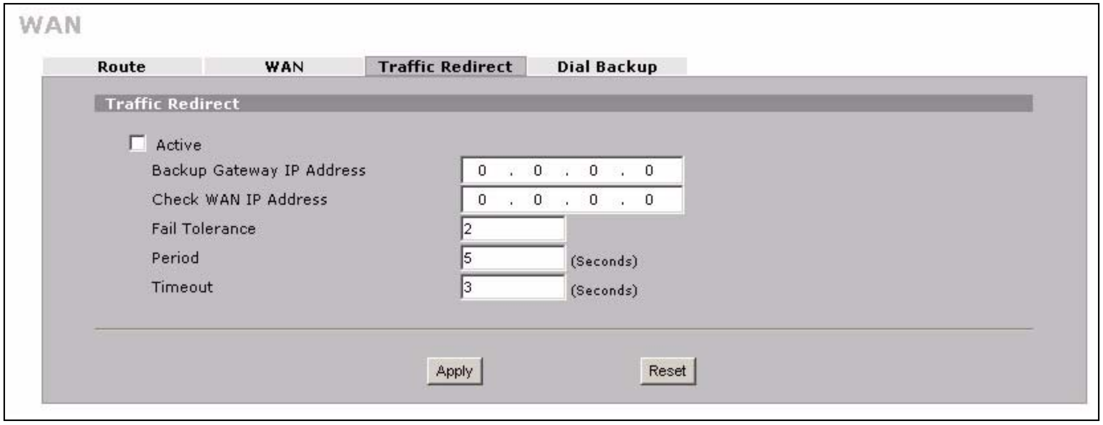
**Figure 107** Traffic Redirect LAN Setup


Subnet 1
192.168.1.0 - 192.168.1.24
WAN
Internet
Gateway
LAN
Backup Gateway
Subnet 2
192.168.2.0 - 192.168.2.24

## 8.9 Configuring Traffic Redirect

To change your ZyWALL's traffic redirect settings, click **NETWORK** > **WAN** > **Traffic Redirect**. The screen appears as shown.

**Figure 108** NETWORK > WAN > Traffic Redirect


WAN
Route
WAN
Traffic Redirect
Dial Backup
Traffic Redirect
Apply
Reset

☐ Active
Backup Gateway IP Address: 0 . 0 . 0 . 0
Check WAN IP Address: 0 . 0 . 0 . 0
Fail Tolerance: 2
Period: 5 (Seconds)
Timeout: 3 (Seconds)

The following table describes the labels in this screen.

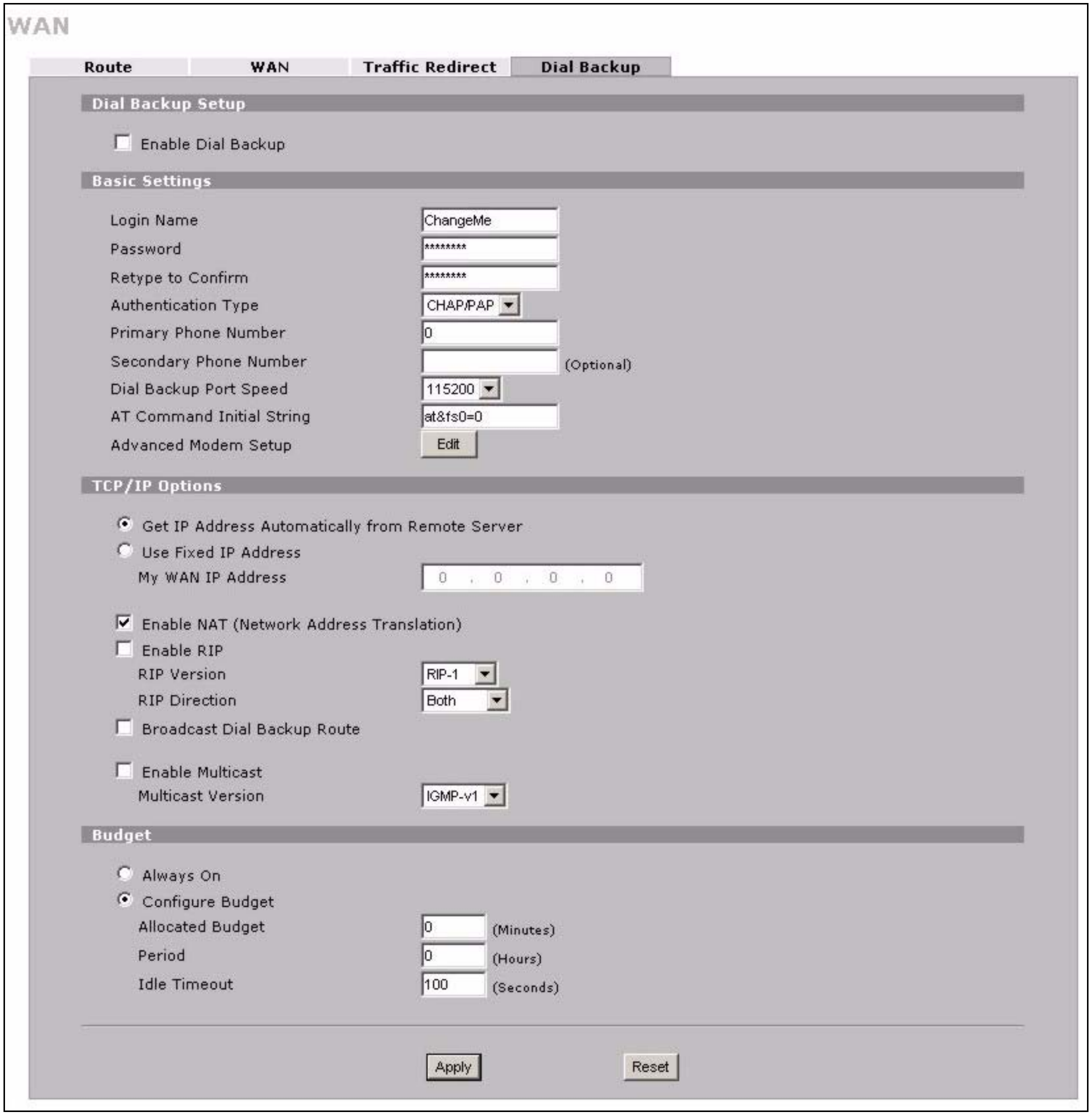
**Table 35** NETWORK > WAN > Traffic Redirect

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to have the ZyWALL use traffic redirect if the normal WAN connection goes down. |
| Backup Gateway IP Address | Type the IP address of your backup gateway in dotted decimal notation. The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates. |
| Check WAN IP Address | Configuration of this field is optional. If you do not enter an IP address here, the ZyWALL will use the default gateway IP address. Configure this field to test your ZyWALL's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). |
| Fail Tolerance | Type how many WAN connection checks can fail (1 to 10) before the connection is considered "down" (not connected). The ZyWALL still checks a "down" connection to detect if it reconnects. |
| Period | The ZyWALL tests a WAN connection by periodically sending a ping to either the default gateway or the address in the **Check WAN IP Address** field.<br>Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic. |
| Timeout | Type the number of seconds (1 to 10) for your ZyWALL to wait for a response to the ping before considering the check to have failed. This setting must be less than the **Period**. Use a higher value in this field if your network is busy or congested. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.10 Configuring Dial Backup

Click **NETWORK** > **WAN** > **Dial Backup** to display the **Dial Backup** screen. Use this screen to configure the backup WAN dial-up connection.

**Figure 109** NETWORK > WAN > Dial Backup



Dial Backup Setup

☐ Enable Dial Backup

Basic Settings

| | |
|---|---|
| Login Name | ChangeMe |
| Password | ******** |
| Retype to Confirm | ******** |
| Authentication Type | CHAP/PAP |
| Primary Phone Number | 0 |
| Secondary Phone Number | (Optional) |
| Dial Backup Port Speed | 115200 |
| AT Command Initial String | at&fs0=0 |
| Advanced Modem Setup | Edit |

TCP/IP Options

● Get IP Address Automatically from Remote Server
○ Use Fixed IP Address
My WAN IP Address 0 . 0 . 0 . 0

☑ Enable NAT (Network Address Translation)
☐ Enable RIP
RIP Version RIP-1
RIP Direction Both
☐ Broadcast Dial Backup Route

☐ Enable Multicast
Multicast Version IGMP-v1

Budget

○ Always On
● Configure Budget
Allocated Budget 0 (Minutes)
Period 0 (Hours)
Idle Timeout 100 (Seconds)

The following table describes the labels in this screen.

**Table 36** NETWORK > WAN > Dial Backup

| LABEL | DESCRIPTION |
|---|---|
| Dial Backup Setup | |
| Enable Dial Backup | Select this check box to turn on dial backup. |
| Basic Settings | |
| Login Name | Type the login name assigned by your ISP. |
| Password | Type the password assigned by your ISP. |
| Retype to Confirm | Type your password again to make sure that you have entered is correctly. |
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your ZyWALL accepts CHAP only.<br>**PAP** - Your ZyWALL accepts PAP only. |

**Table 36** NETWORK > WAN > Dial Backup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Primary/ Secondary Phone Number | Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required. |
| Dial Backup Port Speed | Use the drop-down list box to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps. |
| AT Command Initial String | Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands. |
| Advanced Modem Setup | Click **Edit** to display the **Advanced Setup** screen and edit the details of your dial backup setup. |
| TCP/IP Options | |
| Get IP Address Automatically from Remote Server | Type the login name assigned by your ISP for this remote node. |
| Used Fixed IP Address | Select this check box if your ISP assigned you a fixed IP address, then enter the IP address in the following field. |
| My WAN IP Address | Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Type your WAN IP address here if you know it (static). This is the address assigned to your local ZyWALL, not the remote router. |
| Enable NAT (Network Address Translation) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network.<br>Select the check box to enable NAT. Clear the check box to disable NAT so the ZyWALL does not perform any NAT mapping for the dial backup connection. |
| Enable RIP | Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives. |
| Broadcast Dial Backup Route | Select this check box to forward the backup route broadcasts to the WAN. |

**Table 36** NETWORK > WAN > Dial Backup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |
| Multicast Version | Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*. |
| Budget | |
| Always On | Select this check box to have the dial backup connection on all of the time. |
| Configure Budget | Select this check box to have the dial backup connection on during the time that you select. |
| Allocated Budget | Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field. |
| Period | Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour). |
| Idle Timeout | Type the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) for the ZyWALL to wait before it automatically disconnects the dial backup connection. This option applies only when the ZyWALL initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting **Always On**). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.11 Advanced Modem Setup

### 8.11.1 AT Command Strings

For regular telephone lines, the default Dial string tells the modem that the line uses tone dialing. `ATDT` is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to `ATDP`.

For ISDN lines, there are many more protocols and operational modes. Please consult the documentation of your TA. You may need additional commands in both Dial and Init strings.

### 8.11.2 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the Drop DTR When Hang Up check box is selected, the ZyWALL uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command `ATH`.

### 8.11.3 Response Strings

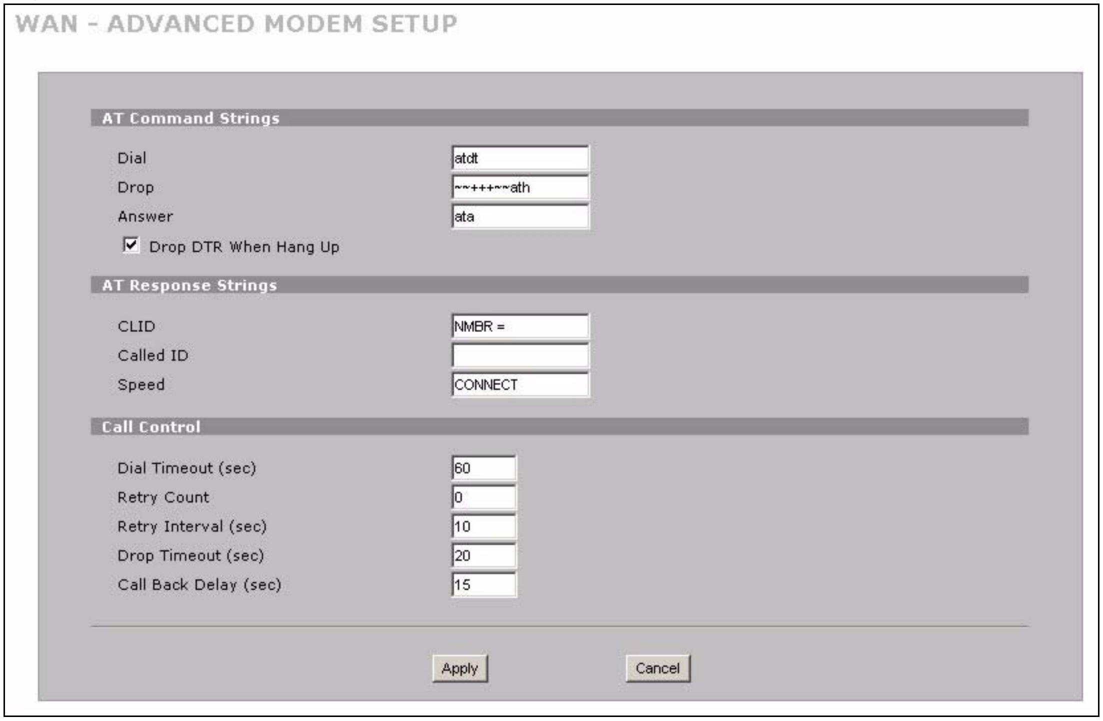
The response strings tell the ZyWALL the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

## 8.12 Configuring Advanced Modem Setup

Click the **Edit** button in the **Dial Backup** screen to display the **Advanced Setup** screen.

Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

**Figure 110** NETWORK > WAN > Dial Backup > Edit



Dial: atdt
Drop: ~~+++~~ath
Answer: ata
☑ Drop DTR When Hang Up
CLID: NMBR =
Called ID:
Speed: CONNECT
Dial Timeout (sec): 60
Retry Count: 0
Retry Interval (sec): 10
Drop Timeout (sec): 20
Call Back Delay (sec): 15

The following table describes the labels in this screen.

**Table 37** NETWORK > WAN > Dial Backup > Edit

| LABEL | DESCRIPTION |
|---|---|
| AT Command Strings | |
| Dial | Type the AT Command string to make a call. |
| Drop | Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~~+++~~ath" can be used if your modem has a slow response time. |
| Answer | Type the AT Command string to answer a call. |

**Table 37** NETWORK > WAN > Dial Backup > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Drop DTR When Hang Up | Select this check box to have the ZyWALL drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out. |
| AT Response Strings | |
| CLID | Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication. |
| Called ID | Type the keyword preceding the dialed number. |
| Speed | Type the keyword preceding the connection speed. |
| Call Control | |
| Dial Timeout (sec) | Type a number of seconds for the ZyWALL to try to set up an outgoing call before timing out (stopping). |
| Retry Count | Type a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number. |
| Retry Interval (sec) | Type a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted. |
| Drop Timeout (sec) | Type the number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation. |
| Call Back Delay (sec) | Type a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the corresponding callback call. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 9

# DMZ Screens

This chapter describes how to configure the ZyWALL's DMZ.

## 9.1 DMZ

The DeMilitarized Zone (DMZ) provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

It is highly recommended that you connect all of your public servers to the DMZ port(s).

It is also highly recommended that you keep all sensitive information off of the public servers connected to the DMZ port. Store sensitive information on LAN computers.

## 9.2 Configuring DMZ

The DMZ and the connected computers can have private or public IP addresses.

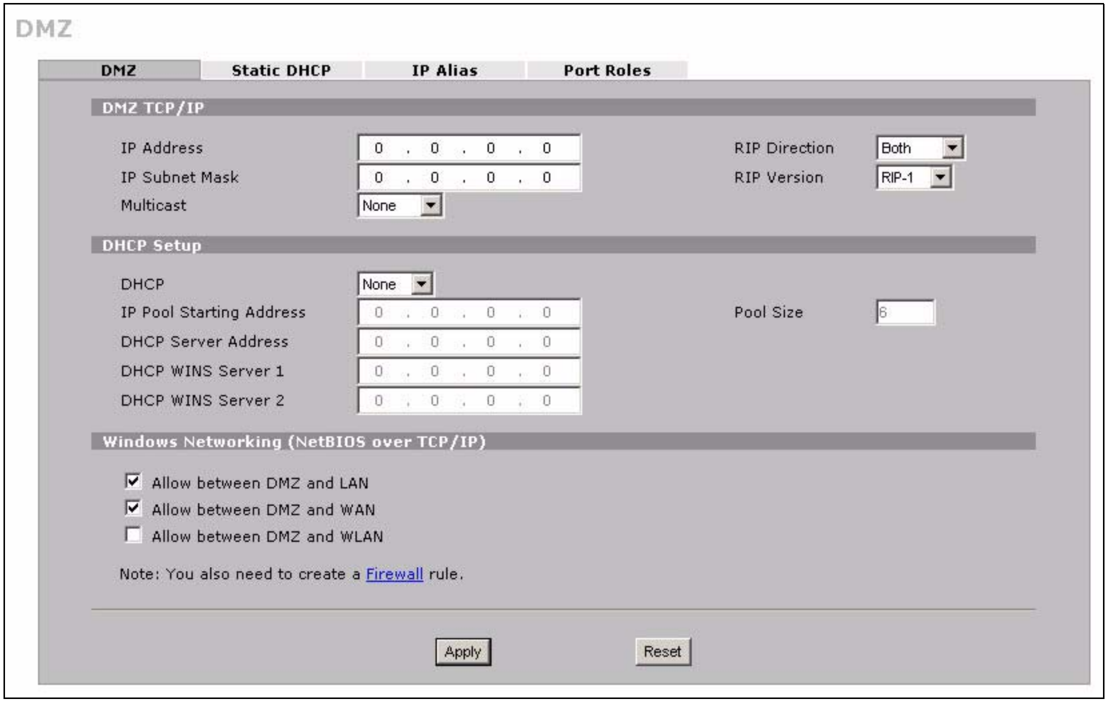
When the DMZ uses public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See Appendix C on page 645 for information on IP subnetting. If you do not configure SUA NAT or any full feature NAT mapping rules for the public IP addresses on the DMZ, the ZyWALL will route traffic to the public IP addresses on the DMZ without performing NAT. This may be useful for hosting servers for NAT unfriendly applications (see Chapter 17 on page 331 for more information).

If the DMZ computers use private IP addresses, use NAT if you want to make them publicly accessible.

Like the LAN, the ZyWALL can also assign TCP/IP configuration via DHCP to computers connected to the DMZ ports.

From the main menu, click **NETWORK** > **DMZ** to open the **DMZ** screen. The screen appears as shown next.

**Figure 111** NETWORK > DMZ



DMZ TCP/IP

IP Address: 0 . 0 . 0 . 0
IP Subnet Mask: 0 . 0 . 0 . 0
Multicast: None
RIP Direction: Both
RIP Version: RIP-1

DHCP Setup

DHCP: None
IP Pool Starting Address: 0 . 0 . 0 . 0
Pool Size: 6
DHCP Server Address: 0 . 0 . 0 . 0
DHCP WINS Server 1: 0 . 0 . 0 . 0
DHCP WINS Server 2: 0 . 0 . 0 . 0

Windows Networking (NetBIOS over TCP/IP)

☑ Allow between DMZ and LAN
☑ Allow between DMZ and WAN
☐ Allow between DMZ and WLAN

Note: You also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 38** NETWORK > DMZ

| LABEL | DESCRIPTION |
|---|---|
| DMZ TCP/IP | |
| IP Address | Type the IP address of your ZyWALL's DMZ port in dotted decimal notation.<br>Note: Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL 255.255.255.0. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |

**Table 38** NETWORK > DMZ (continued)

| LABEL | DESCRIPTION |
|---|---|
| Multicast | Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*. |
| DHCP Setup | |
| DHCP | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields.<br>Select **Relay** to have the ZyWALL forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field.<br>Select **None** to stop the ZyWALL from acting as a DHCP server. When you select **None**, you must have another DHCP server on your LAN, or else the computers must be manually configured. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| DHCP Server Address | Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| DHCP WINS Server 1, 2 | Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. |
| Windows Networking (NetBIOS over TCP/IP) | |
| Allow between DMZ and LAN | Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to configure a DMZ to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN. |
| Allow between DMZ and WAN | Select this check box to forward NetBIOS packets from the DMZ to the WAN and from the WAN to the DMZ.<br>Clear this check box to block all NetBIOS packets going from the DMZ to the WAN and from the WAN to the DMZ. |
| Allow between DMZ and WLAN | Select this check box to forward NetBIOS packets from the WLAN to the DMZ and from the DMZ to the WLAN. If your firewall is enabled with the default policy set to block DMZ to WLAN traffic and WLAN to DMZ traffic, you also need to configure DMZ to WLAN and WLAN to DMZ firewall rules that forward NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the WLAN to the DMZ and from the DMZ to the WLAN. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

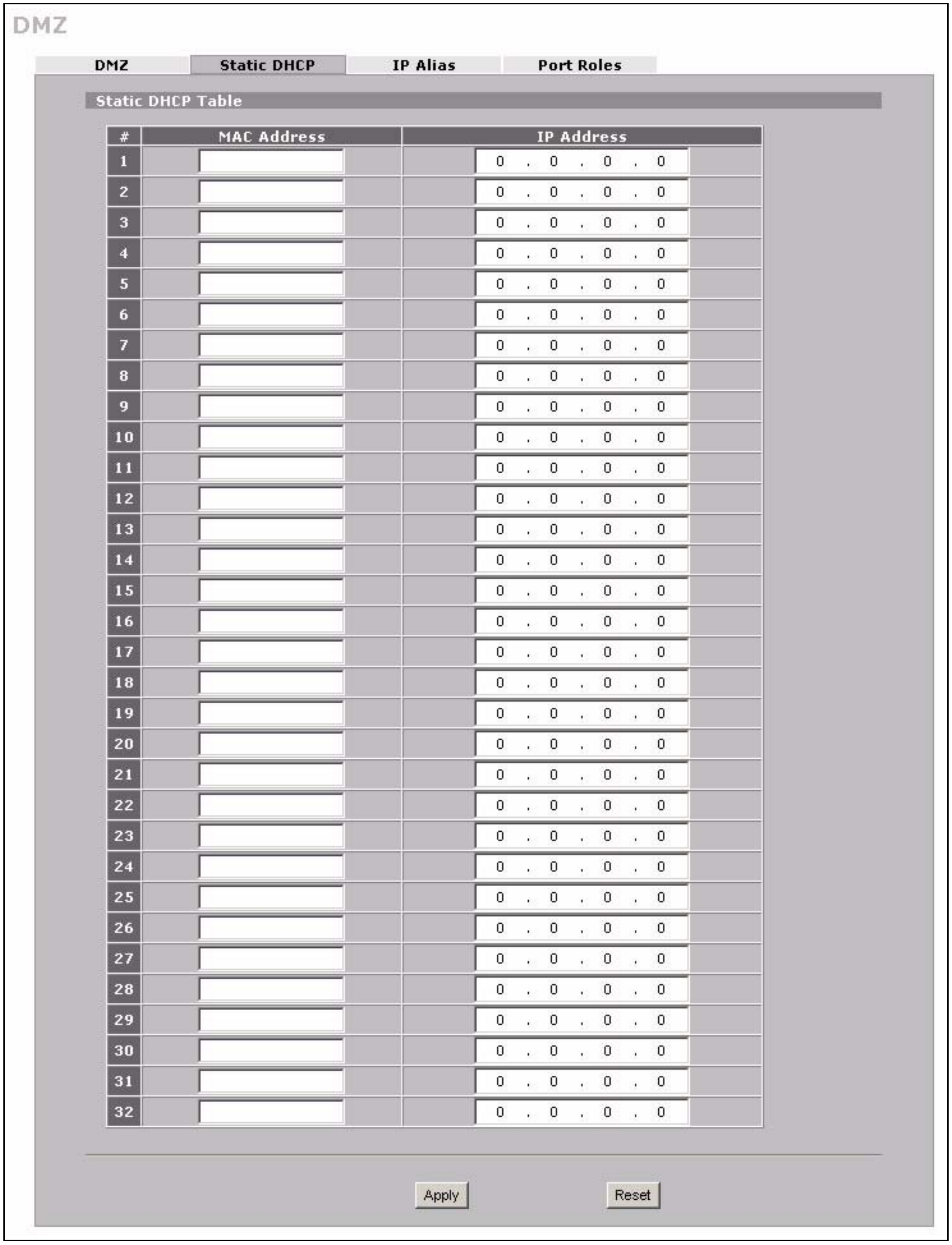
## 9.3 DMZ Static DHCP

This table allows you to assign IP addresses on the DMZ to specific individual computers based on their MAC addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your ZyWALL’s static DHCP settings on the DMZ, click **NETWORK** > **DMZ** > **Static DHCP**. The screen appears as shown.

**Figure 112** NETWORK > DMZ > Static DHCP



| # | MAC Address | IP Address |
|---|---|---|
| 1 | | 0 . 0 . 0 . 0 |
| 2 | | 0 . 0 . 0 . 0 |
| 3 | | 0 . 0 . 0 . 0 |
| 4 | | 0 . 0 . 0 . 0 |
| 5 | | 0 . 0 . 0 . 0 |
| 6 | | 0 . 0 . 0 . 0 |
| 7 | | 0 . 0 . 0 . 0 |
| 8 | | 0 . 0 . 0 . 0 |
| 9 | | 0 . 0 . 0 . 0 |
| 10 | | 0 . 0 . 0 . 0 |
| 11 | | 0 . 0 . 0 . 0 |
| 12 | | 0 . 0 . 0 . 0 |
| 13 | | 0 . 0 . 0 . 0 |
| 14 | | 0 . 0 . 0 . 0 |
| 15 | | 0 . 0 . 0 . 0 |
| 16 | | 0 . 0 . 0 . 0 |
| 17 | | 0 . 0 . 0 . 0 |
| 18 | | 0 . 0 . 0 . 0 |
| 19 | | 0 . 0 . 0 . 0 |
| 20 | | 0 . 0 . 0 . 0 |
| 21 | | 0 . 0 . 0 . 0 |
| 22 | | 0 . 0 . 0 . 0 |
| 23 | | 0 . 0 . 0 . 0 |
| 24 | | 0 . 0 . 0 . 0 |
| 25 | | 0 . 0 . 0 . 0 |
| 26 | | 0 . 0 . 0 . 0 |
| 27 | | 0 . 0 . 0 . 0 |
| 28 | | 0 . 0 . 0 . 0 |
| 29 | | 0 . 0 . 0 . 0 |
| 30 | | 0 . 0 . 0 . 0 |
| 31 | | 0 . 0 . 0 . 0 |
| 32 | | 0 . 0 . 0 . 0 |

The following table describes the labels in this screen.

**Table 39** NETWORK > DMZ > Static DHCP

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the Static IP table entry (row). |
| MAC Address | Type the MAC address of a computer on your DMZ. |
| IP Address | Type the IP address that you want to assign to the computer on your DMZ.<br>Alternatively, click the right mouse button to copy and/or paste the IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.4 DMZ IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

The ZyWALL has a single DMZ interface. Even though more than one of ports 1~4 may be in the DMZ port role, they are all still part of a single physical Ethernet interface and all use the same IP address.

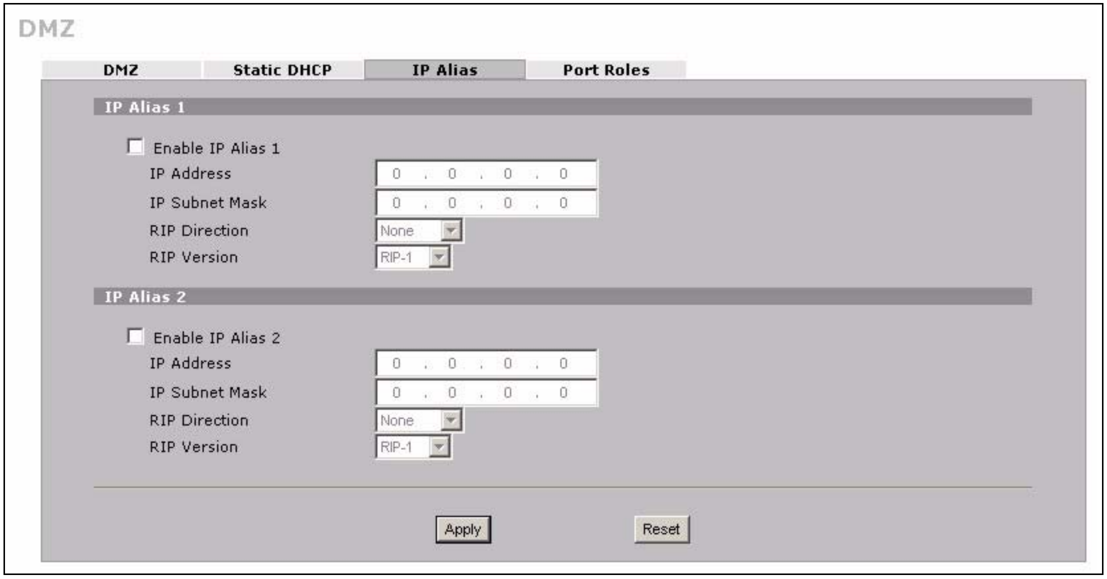
The ZyWALL supports three logical DMZ interfaces via its single physical DMZ Ethernet interface. The ZyWALL itself is the gateway for each of the logical DMZ networks.

The IP alias IP addresses can be either private or public regardless of whether the physical DMZ interface is set to use a private or public IP address. Use NAT if you want to make DMZ computers with private IP addresses publicly accessible (see Chapter 17 on page 331 for more information). When you use IP alias, you can have the DMZ use both public and private IP addresses at the same time.

Make sure that the subnets of the logical networks do not overlap.

To change your ZyWALL's IP alias settings, click **NETWORK** > **DMZ** > **IP Alias**. The screen appears as shown.

**Figure 113** NETWORK > DMZ > IP Alias


DMZ
DMZ
Static DHCP
IP Alias
Port Roles
IP Alias 1
☐ Enable IP Alias 1
IP Address
0 . 0 . 0 . 0
IP Subnet Mask
0 . 0 . 0 . 0
RIP Direction
None
RIP Version
RIP-1
IP Alias 2
☐ Enable IP Alias 2
IP Address
0 . 0 . 0 . 0
IP Subnet Mask
0 . 0 . 0 . 0
RIP Direction
None
RIP Version
RIP-1
Apply
Reset

The following table describes the labels in this screen.

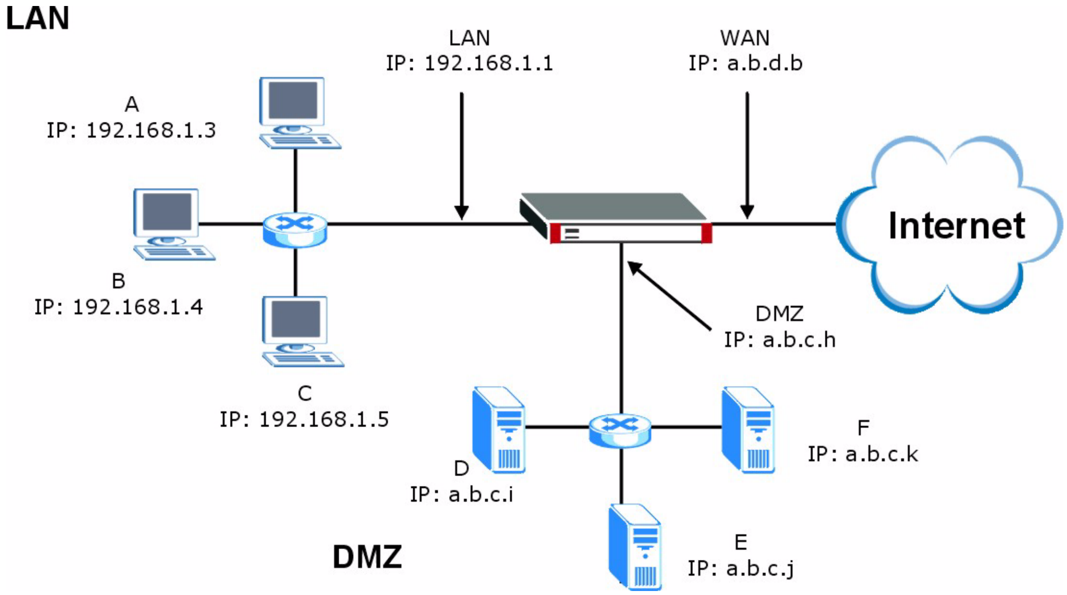
**Table 40** NETWORK > DMZ > IP Alias

| LABEL | DESCRIPTION |
|---|---|
| Enable IP Alias 1, 2 | Select the check box to configure another DMZ network for the ZyWALL. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation.<br>Note: Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets. |
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.5 DMZ Public IP Address Example

The following figure shows a simple network setup with public IP addresses on the WAN and DMZ and private IP addresses on the LAN. Lower case letters represent public IP addresses (like a.b.c.d for example). The LAN port and connected computers (A through C) use private IP addresses that are in one subnet. The DMZ port and connected servers (D through F) use public IP addresses that are in another subnet. The public IP addresses of the DMZ and WAN ports are in separate subnets.

**Figure 114** DMZ Public Address Example

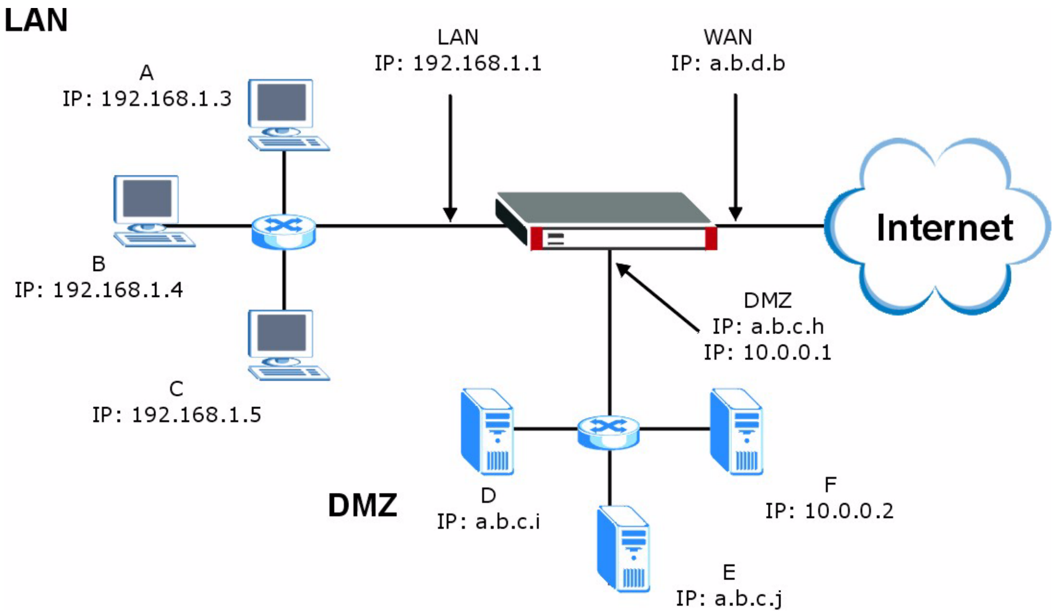


## 9.6 DMZ Private and Public IP Address Example

The following figure shows a network setup with both private and public IP addresses on the DMZ. Lower case letters represent public IP addresses (like a.b.c.d for example). The LAN port and connected computers (A through C) use private IP addresses that are in one subnet. The DMZ port and server F use private IP addresses that are in one subnet. The private IP addresses of the LAN and DMZ are on separate subnets. The DMZ port and connected servers (D and E) use public IP addresses that are in one subnet. The public IP addresses of the DMZ and WAN are on separate subnets.

Configure one subnet (either the public or the private) in the **Network > DMZ** screen (see Figure 9.2 on page 171) and configure the other subnet in the **Network > DMZ > IP Alias** screen (see Figure 9.4 on page 175) to use this kind of network setup. You also need to configure NAT for the private DMZ IP addresses.

**Figure 115** DMZ Private and Public Address Example


LAN
LAN
IP: 192.168.1.1
WAN
IP: a.b.d.b
A
IP: 192.168.1.3
B
IP: 192.168.1.4
C
IP: 192.168.1.5
Internet
DMZ
IP: a.b.c.h
IP: 10.0.0.1
DMZ
D
IP: a.b.c.i
E
IP: a.b.c.j
F
IP: 10.0.0.2

## 9.7 DMZ Port Roles

Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Ports 1~4 on the ZyWALL can be part of the LAN, DMZ or WLAN interface.

Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

1 A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyWALL's LAN, DMZ or WLAN IP address.

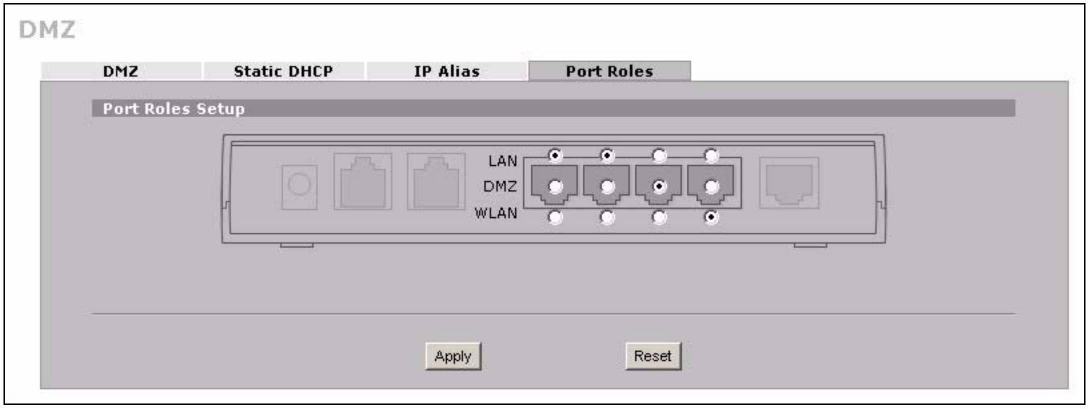
2 Use the appropriate LAN, DMZ or WLAN IP address to access the ZyWALL.

To change your ZyWALL's port role settings, click **NETWORK** > **DMZ** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. On the ZyWALL, ports 1 to 4 are all LAN ports by default.

Your changes are also reflected in the **LAN** and/or **WLAN Port Roles** screens.

**Figure 116** NETWORK > DMZ > Port Roles


DMZ
DMZ
Static DHCP
IP Alias
Port Roles
Port Roles Setup
LAN
DMZ
WLAN
Apply
Reset

The following table describes the labels in this screen.

**Table 41** NETWORK > DMZ > Port Roles

| LABEL | DESCRIPTION |
|---|---|
| LAN | Select a port's LAN radio button to use the port as part of the LAN. The port will use the ZyWALL's LAN IP address and MAC address. |
| DMZ | Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the ZyWALL's DMZ IP address and MAC address. |
| WLAN | Select a port's WLAN radio button to use the port as part of the WLAN.<br>The port will use the ZyWALL's WLAN IP address and MAC address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 10

# Wireless LAN

This chapter discusses how to configure wireless LAN on the ZyWALL.

## 10.1 Wireless LAN Introduction

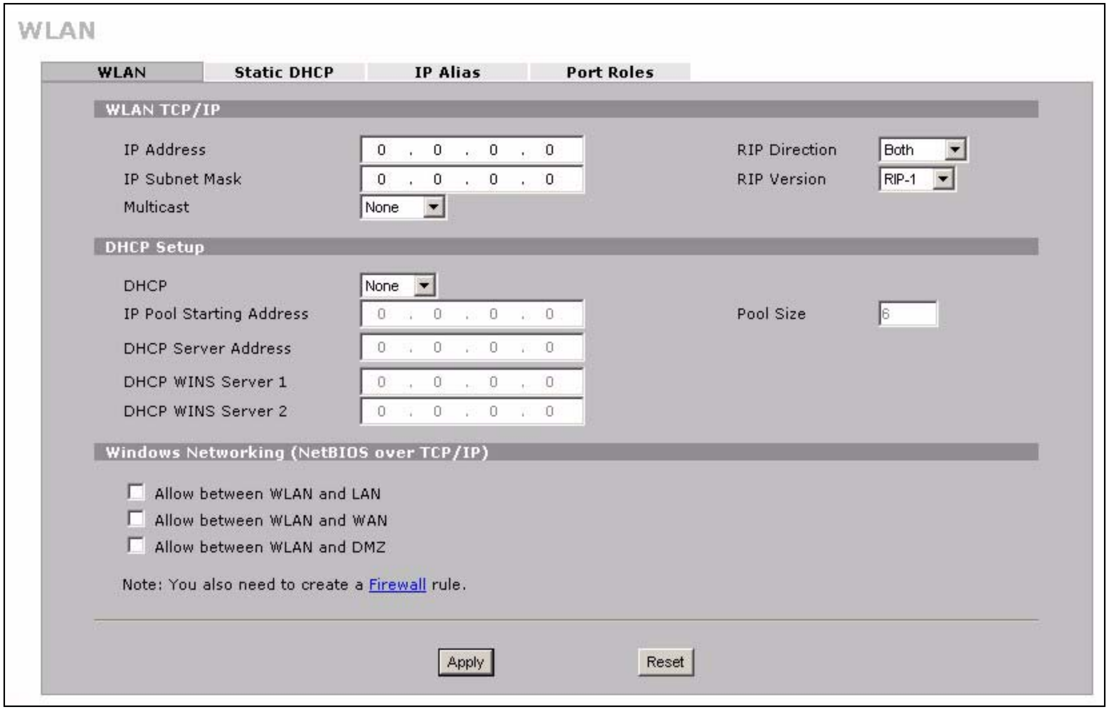
A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN. To add a wireless network to the ZyWALL, you can connect an Access Point to a port in the WLAN role.

## 10.2 Configuring WLAN

To add wireless functionality to the ZyWALL, use the **Port Roles** screen (see Figure 121 on page 188) to set a port to be part of the WLAN and connect an access point (AP) to the WLAN interface.

Click **NETWORK** > **WLAN** to open the **WLAN** screen to configure the IP address for ZyWALL's WLAN interface, other TCP/IP and DHCP settings.

**Figure 117** NETWORK > WLAN



WLAN TCP/IP

IP Address: 0 . 0 . 0 . 0
IP Subnet Mask: 0 . 0 . 0 . 0
Multicast: None
RIP Direction: Both
RIP Version: RIP-1

DHCP Setup

DHCP: None
IP Pool Starting Address: 0 . 0 . 0 . 0
Pool Size: 6
DHCP Server Address: 0 . 0 . 0 . 0
DHCP WINS Server 1: 0 . 0 . 0 . 0
DHCP WINS Server 2: 0 . 0 . 0 . 0

Windows Networking (NetBIOS over TCP/IP)

☐ Allow between WLAN and LAN
☐ Allow between WLAN and WAN
☐ Allow between WLAN and DMZ

Note: You also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 42** NETWORK > WLAN

| LABEL | DESCRIPTION |
|---|---|
| WLAN TCP/IP | |
| IP Address | Type the IP address of your ZyWALL’s WLAN interface in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.<br>Note: Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your ZyWALL automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |

**Table 42** NETWORK > WLAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| Multicast | Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*. |
| DHCP Setup | |
| DHCP | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields.<br>Select **Relay** to have the ZyWALL forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field.<br>Select **None** to stop the ZyWALL from acting as a DHCP server. When you select **None**, you must have another DHCP server on your WLAN, or else the computers must be manually configured. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| DHCP Server Address | Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| DHCP WINS Server 1, 2 | Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. |
| Windows Networking (NetBIOS over TCP/IP) | NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN. |
| Allow between WLAN and LAN | Select this check box to forward NetBIOS packets from the WLAN to the LAN and from the LAN to the WLAN.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WLAN and from the WLAN to the LAN. |
| Allow between WLAN and WAN | Select this check box to forward NetBIOS packets from the WLAN to the WAN and from the WAN to the WLAN.<br>Clear this check box to block all NetBIOS packets going from the WLAN to the WAN and from the WAN to the WLAN. |
| Allow between WLAN and DMZ | Select this check box to forward NetBIOS packets from the WLAN to the DMZ and from the DMZ to the WLAN. If your firewall is enabled with the default policy set to block WLAN to DMZ traffic and DMZ to WLAN traffic, you also need to configure WLAN to DMZ and DMZ to WLAN firewall rules that forward NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the WLAN to the DMZ and from the DMZ to the WLAN. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

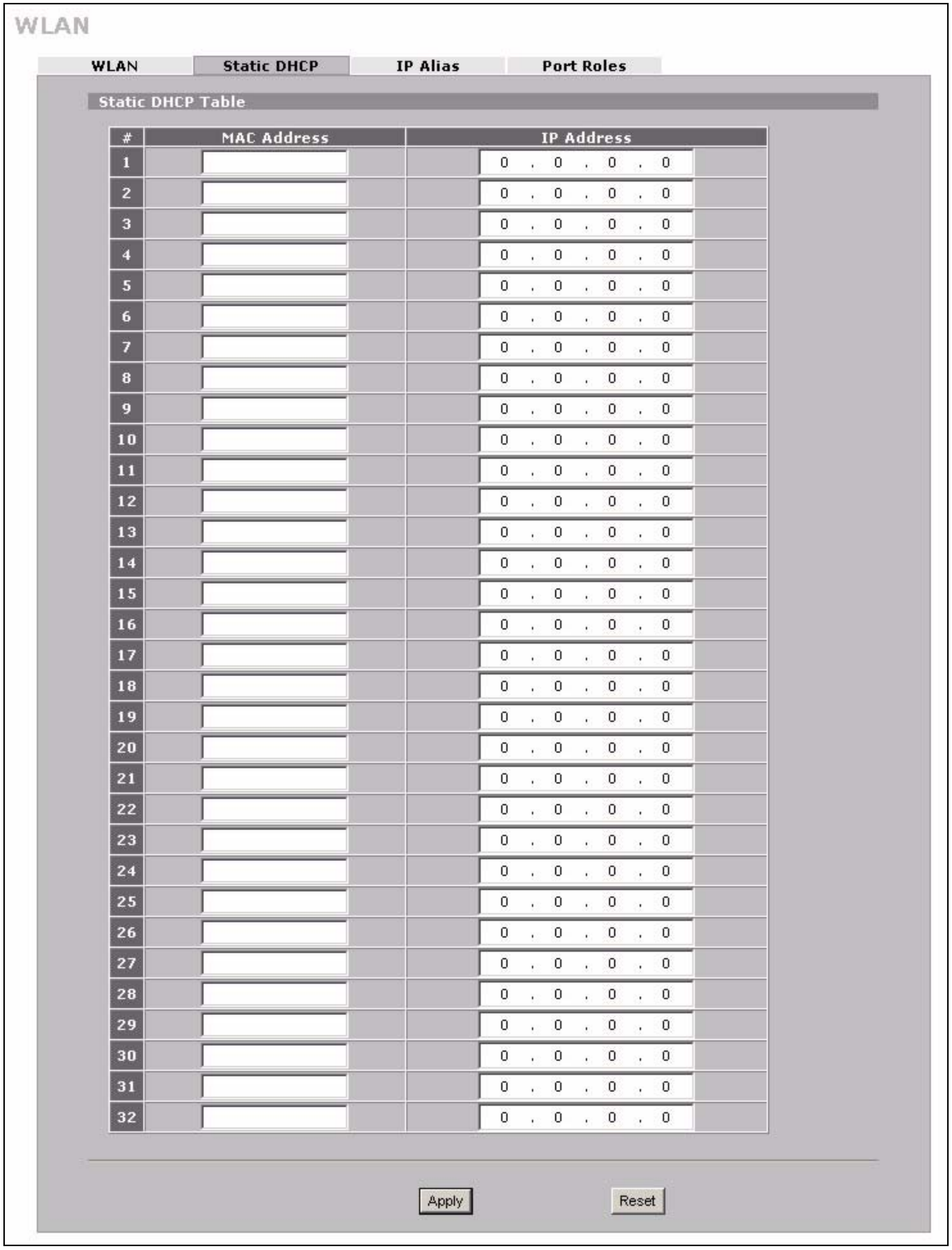
## 10.3 WLAN Static DHCP

This table allows you to assign IP addresses on the WLAN to specific individual computers based on their MAC addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your ZyWALL’s WLAN static DHCP settings, click **NETWORK** >**WLAN** > **Static DHCP**. The screen appears as shown.

**Figure 118** NETWORK > WLAN > Static DHCP



| # | MAC Address | IP Address |
|---|---|---|
| 1 | | 0 . 0 . 0 . 0 |
| 2 | | 0 . 0 . 0 . 0 |
| 3 | | 0 . 0 . 0 . 0 |
| 4 | | 0 . 0 . 0 . 0 |
| 5 | | 0 . 0 . 0 . 0 |
| 6 | | 0 . 0 . 0 . 0 |
| 7 | | 0 . 0 . 0 . 0 |
| 8 | | 0 . 0 . 0 . 0 |
| 9 | | 0 . 0 . 0 . 0 |
| 10 | | 0 . 0 . 0 . 0 |
| 11 | | 0 . 0 . 0 . 0 |
| 12 | | 0 . 0 . 0 . 0 |
| 13 | | 0 . 0 . 0 . 0 |
| 14 | | 0 . 0 . 0 . 0 |
| 15 | | 0 . 0 . 0 . 0 |
| 16 | | 0 . 0 . 0 . 0 |
| 17 | | 0 . 0 . 0 . 0 |
| 18 | | 0 . 0 . 0 . 0 |
| 19 | | 0 . 0 . 0 . 0 |
| 20 | | 0 . 0 . 0 . 0 |
| 21 | | 0 . 0 . 0 . 0 |
| 22 | | 0 . 0 . 0 . 0 |
| 23 | | 0 . 0 . 0 . 0 |
| 24 | | 0 . 0 . 0 . 0 |
| 25 | | 0 . 0 . 0 . 0 |
| 26 | | 0 . 0 . 0 . 0 |
| 27 | | 0 . 0 . 0 . 0 |
| 28 | | 0 . 0 . 0 . 0 |
| 29 | | 0 . 0 . 0 . 0 |
| 30 | | 0 . 0 . 0 . 0 |
| 31 | | 0 . 0 . 0 . 0 |
| 32 | | 0 . 0 . 0 . 0 |

The following table describes the labels in this screen.

**Table 43** NETWORK > WLAN > Static DHCP

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the Static IP table entry (row). |
| MAC Address | Type the MAC address of a computer on your WLAN. |
| IP Address | Type the IP address that you want to assign to the computer on your WLAN.<br>Alternatively, click the right mouse button to copy and/or paste the IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.4 WLAN IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

The ZyWALL has a single WLAN interface. Even though more than one of ports 1~4 may be in the WLAN port role, they are all still part of a single physical Ethernet interface and all use the same IP address.

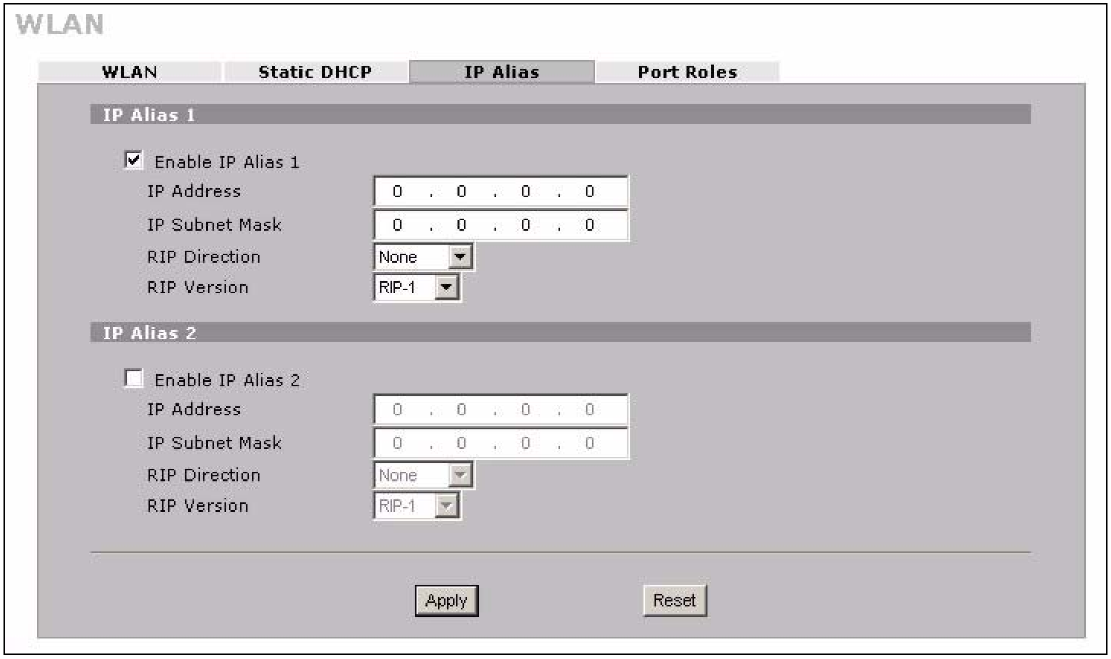
The ZyWALL supports three logical WLAN interfaces via its single physical WLAN Ethernet interface. The ZyWALL itself is the gateway for each of the logical WLAN networks.

When you use IP alias, you can also configure firewall rules to control access between the WLAN's logical networks (subnets).

Make sure that the subnets of the logical networks do not overlap.

To change your ZyWALL's IP alias settings, click **NETWORK** > **WLAN** > **IP Alias**. The screen appears as shown.

**Figure 119** NETWORK > WLAN > IP Alias



IP Alias 1

☑ Enable IP Alias 1
IP Address 0 . 0 . 0 . 0
IP Subnet Mask 0 . 0 . 0 . 0
RIP Direction None
RIP Version RIP-1

IP Alias 2

☐ Enable IP Alias 2
IP Address 0 . 0 . 0 . 0
IP Subnet Mask 0 . 0 . 0 . 0
RIP Direction None
RIP Version RIP-1

The following table describes the labels in this screen.

**Table 44** NETWORK > WLAN > IP Alias

| LABEL | DESCRIPTION |
|---|---|
| Enable IP Alias 1, 2 | Select the check box to configure another WLAN network for the ZyWALL. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation.<br>Alternatively, click the right mouse button to copy and/or paste the IP address. |
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.5 WLAN Port Roles

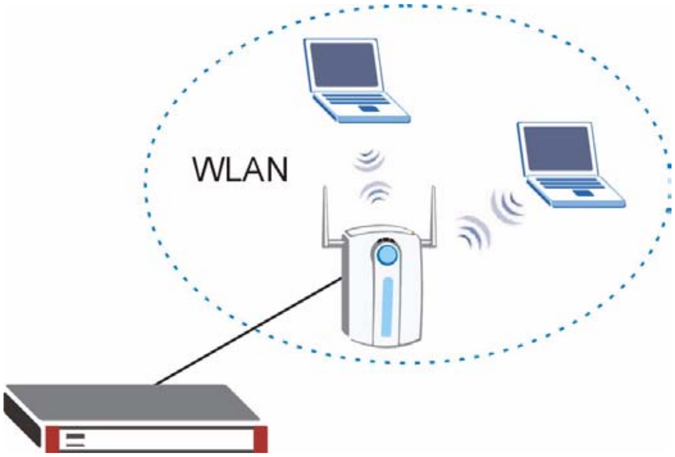
Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Ports 1~4 on the ZyWALL can be part of the LAN, DMZ or WLAN interface.

Connect wireless LAN Access Points (APs) to WLAN interfaces to extend the ZyWALL's wireless LAN coverage. The WLAN port role allows the ZyWALL's firewall to treat traffic from connected APs as part of the ZyWALL's WLAN. You can specify firewall rules for traffic going to or from the WLAN. The WLAN includes the Ethernet ports in the WLAN port role.

The following figure shows the ZyWALL with an AP connected to an Ethernet port in the WLAN port role.

**Figure 120** WLAN Port Role Example



Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

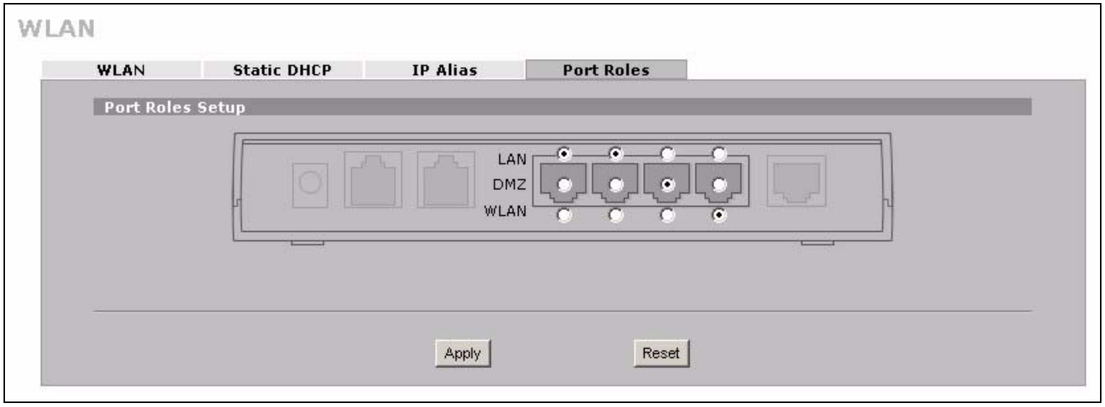
1. A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyWALL's LAN, DMZ or WLAN IP address.
2. Use the appropriate LAN, DMZ or WLAN IP address to access the ZyWALL.

To change your ZyWALL's port role settings, click **NETWORK** > **WLAN** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. On the ZyWALL, ports 1 to 4 are all LAN ports by default.

Your changes are also reflected in the **LAN** and **DMZ Port Roles** screen.

**Figure 121** NETWORK > WLAN > Port Roles



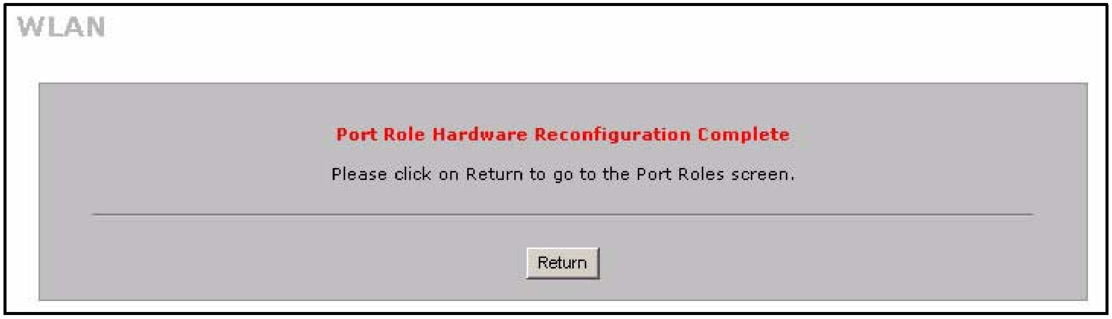
The following table describes the labels in this screen.

**Table 45** NETWORK > WLAN > Port Roles

| LABEL | DESCRIPTION |
|---|---|
| LAN | Select a port's LAN radio button to use the port as part of the LAN. The port will use the LAN IP address. |
| DMZ | Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the DMZ IP address. |
| WLAN | Select a port's WLAN radio button to use the port as part of the WLAN.<br>The port will use the WLAN IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

After you change the LAN/DMZ/WLAN port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

**Figure 122** NETWORK > WLAN > Port Roles: Change Complete



Port Role Hardware Reconfiguration Complete

Please click on Return to go to the Port Roles screen.

# PART III

# Security

Firewall (191)
Content Filtering Screens (223)
Content Filtering Reports (245)
IPSec VPN (253)
Certificates (295)
Authentication Server (323)

# 11

# Firewall

This chapter shows you how to configure your ZyWALL’s firewall.

## 11.1 Firewall Overview

The networking term firewall is a system or group of systems that enforces an access-control policy between two networks. It is generally a mechanism used to protect a trusted network from an untrusted network.

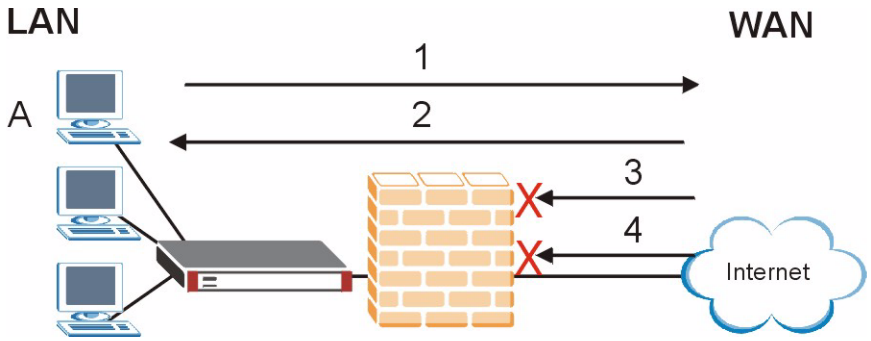
The ZyWALL physically separates the LAN, DMZ, WLAN and the WAN and acts as a secure gateway for all data passing between the networks. The ZyWALL protects against Denial of Service (DoS) attacks, prevents theft, destruction and modification of data, and logs events.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN, DMZ, WLAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.
- allows traffic that originates on the WLAN to go to the WAN.
- allows traffic that originates on the WAN to go to the DMZ and protects your DMZ computers against DoS attacks.
- allows VPN traffic between any of the networks.

The following figure illustrates the default firewall action. User A can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

**Figure 123** Default Firewall Action



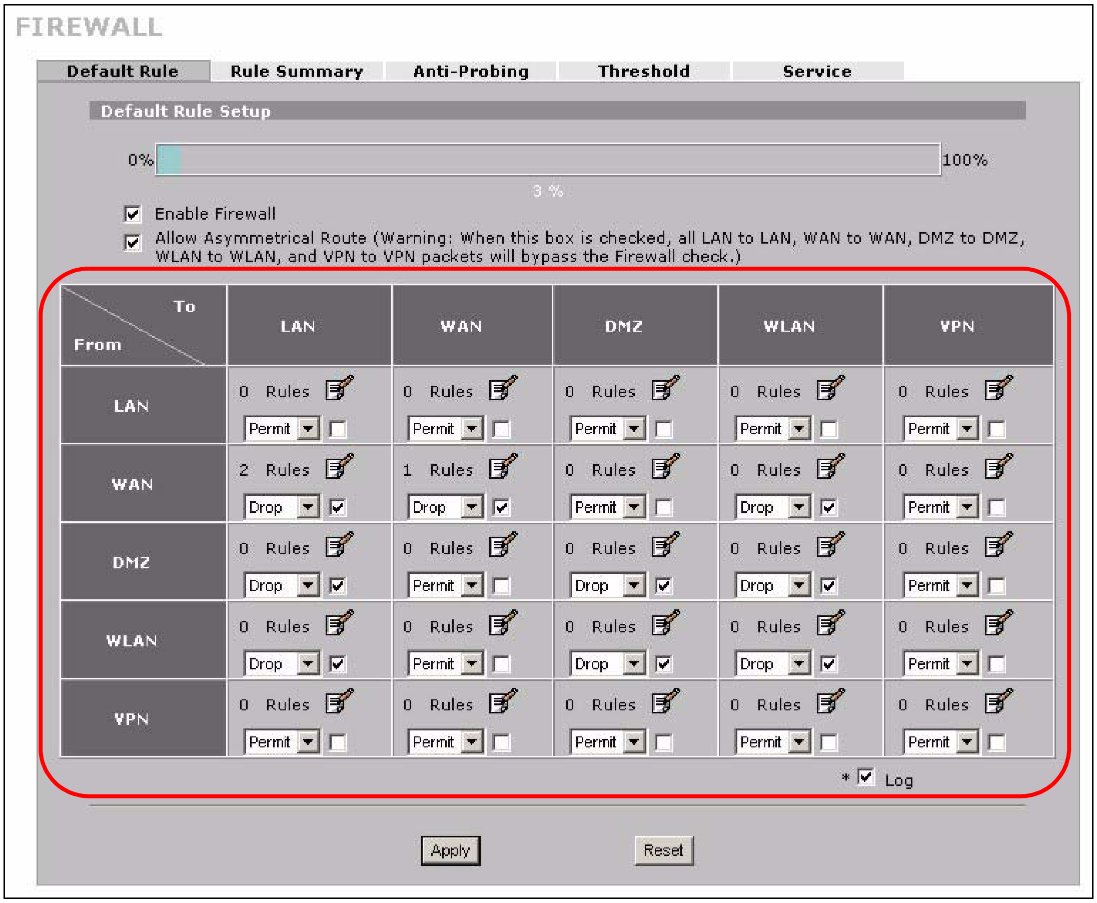
Your customized rules take precedence and override the ZyWALL's default settings. The ZyWALL checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyWALL takes the action specified in the rule.

## 11.2 Packet Direction Matrix

The ZyWALL's packet direction matrix allows you to apply certain security settings (like firewall) to traffic flowing in specific directions.

For example, click **SECURITY** > **FIREWALL** to open the following screen. This screen configures general firewall settings.

**Figure 124** SECURITY > FIREWALL > Default Rule (Router Mode)



☑ Enable Firewall

☑ Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ, WLAN to WLAN, and VPN to VPN packets will bypass the Firewall check.)

| From \ To | LAN | WAN | DMZ | WLAN | VPN |
|---|---|---|---|---|---|
| LAN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |
| WAN | 2 Rules<br>Drop ☑ | 1 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| DMZ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| WLAN | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| VPN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |

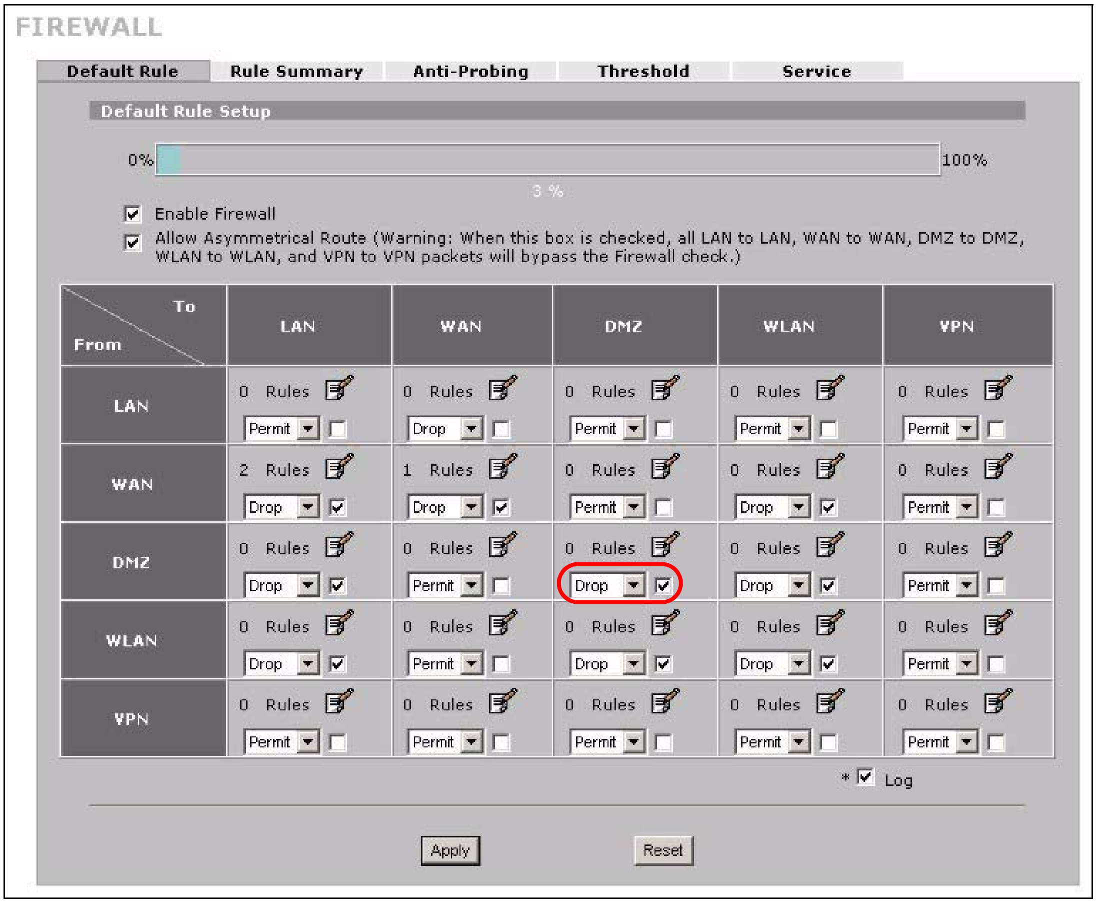
* ☑ Log

Packets have a source and a destination. The packet direction matrix in the lower part of the screen sets what the ZyWALL does with packets traveling in a specific direction that do not match any of the firewall rules.

| From | To |
|---|---|
| A specific interface or any of the ZyWALL's VPN connections | A specific interface or any of the ZyWALL's VPN connections |

To set the ZyWALL to by default silently block traffic from the WAN from going to the DMZ interfaces, you would find where the **From WAN** row and the **To DMZ** column intersect and set the field to **Drop** as shown.

**Figure 125** Default Block Traffic From WAN to DMZ Example



☑ Enable Firewall

☑ Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ, WLAN to WLAN, and VPN to VPN packets will bypass the Firewall check.)

| From \ To | LAN | WAN | DMZ | WLAN | VPN |
|---|---|---|---|---|---|
| LAN | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |
| WAN | 2 Rules<br>Drop ☑ | 1 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| DMZ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| WLAN | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| VPN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |

* ☑ Log

## 11.3 Packet Direction Examples

Firewall rules are grouped based on the direction of travel of packets to which they apply. This section gives some examples of why you might configure firewall rules for specific connection directions.

By default, the ZyWALL allows packets traveling in the following directions.:

- LAN to LAN These rules specify which computers on the LAN can manage the ZyWALL (remote management) and communicate between networks or subnets connected to the LAN interface (IP alias).

> You can also configure the remote management settings to allow only a specific computer to manage the ZyWALL.

- LAN to WAN These rules specify which computers on the LAN can access which computers or services connected to the WAN. See Section 11.5 on page 200 for an example.

By default, the ZyWALL drops packets traveling in the following directions.

- WAN to LAN These rules specify which computers connected to the WAN can access which computers or services on the LAN. For example, you may create rules to:
    - Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
    - Allow public access to a Web server on your protected network. You could also block certain IP addresses from accessing it.

> You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN. See Section 17.5.3 on page 341 for an example.

| | |
|---|---|
| • WAN to WAN | By default the ZyWALL stops computers connected to the WAN from managing the ZyWALL or using the ZyWALL as a gateway to communicate with other computers on the WAN. You could configure one of these rules to allow a WAN computer to manage the ZyWALL. |

You also need to configure the remote management settings to allow a WAN computer to manage the ZyWALL.

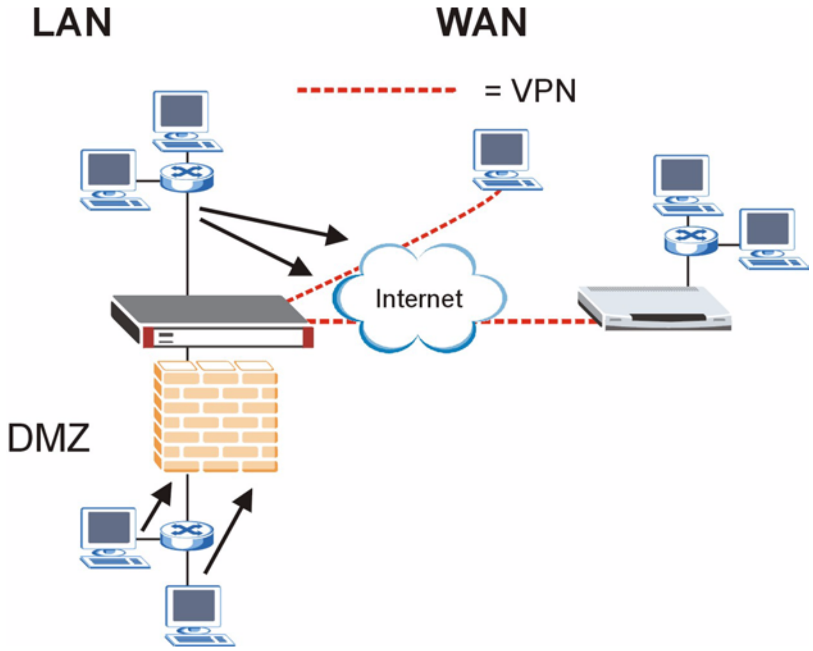
See Chapter 4 on page 89 for information about packets traveling to or from the VPN tunnels.

## 11.3.1 To VPN Packet Direction

The ZyWALL can apply firewall rules to traffic before encrypting it to send through a VPN tunnel. **To VPN** means traffic that comes in through the selected "from" interface and goes out through any of the ZyWALL's VPN tunnels. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through any of the ZyWALL's VPN tunnels.

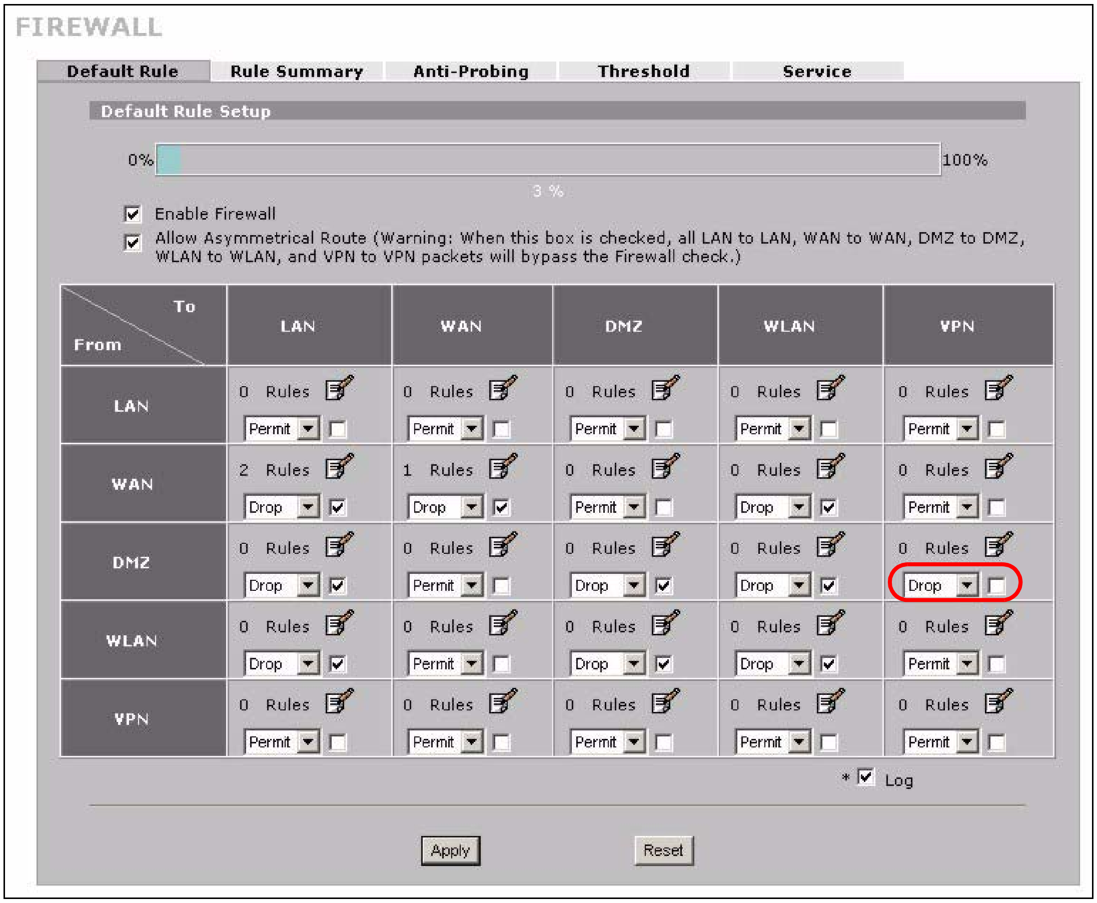
For example, by default the **From LAN To VPN** default firewall rule allows traffic from the LAN computers to go out through any of the ZyWALL's VPN tunnels. You could configure the **From DMZ To VPN** default rule to set the ZyWALL to silently block traffic from the DMZ computers from going out through any of the ZyWALL's VPN tunnels.

**Figure 126** From LAN to VPN Example



In order to do this, you would configure the **SECURITY** > **FIREWALL** > **Default Rule** screen as follows.

**Figure 127** Block DMZ to VPN Traffic by Default Example



☑ Enable Firewall

☑ Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ, WLAN to WLAN, and VPN to VPN packets will bypass the Firewall check.)

| To / From | LAN | WAN | DMZ | WLAN | VPN |
|---|---|---|---|---|---|
| LAN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |
| WAN | 2 Rules<br>Drop ☑ | 1 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| DMZ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☐ |
| WLAN | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| VPN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |

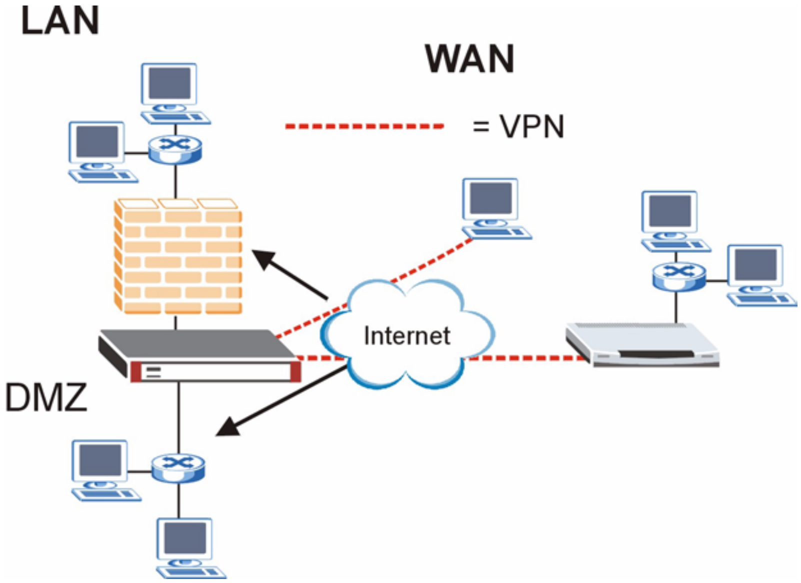
* ☑ Log

## 11.3.2 From VPN Packet Direction

You can also apply firewall rules to traffic that comes in through the ZyWALL’s VPN tunnels. The ZyWALL decrypts the VPN traffic and then applies the firewall rules. **From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected “to” interface.

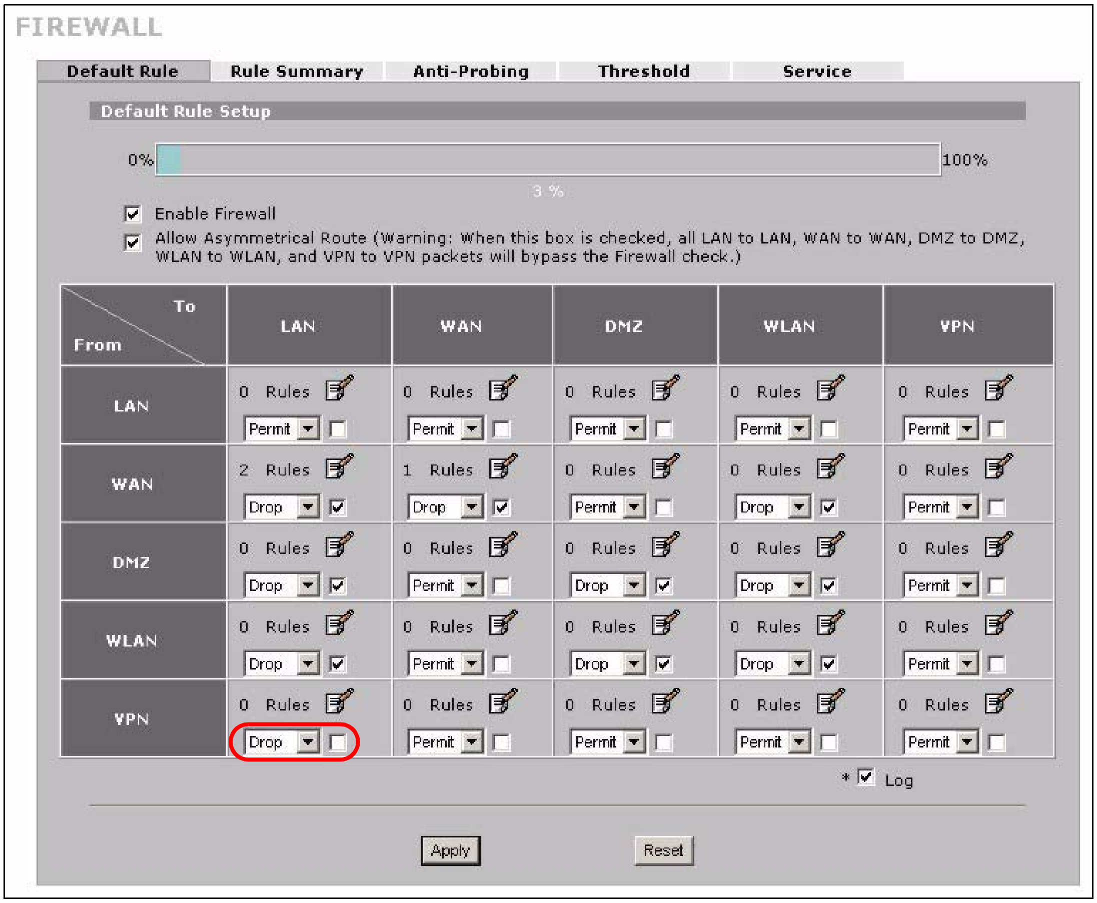
For example, by default the firewall allows traffic from any VPN tunnel to go to any of the ZyWALL’s interfaces, the ZyWALL itself and other VPN tunnels. You could edit the **From VPN To LAN** default firewall rule to silently block traffic from the VPN tunnels from going to the LAN computers.

**Figure 128** From VPN to LAN Example


LAN
WAN
= VPN
Internet
DMZ

In order to do this, you would configure the **SECURITY** > **FIREWALL** > **Default Rule** screen as follows.

**Figure 129** Block VPN to LAN Traffic by Default Example


FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Default Rule Setup
0%
100%
3 %
Apply
Reset

☑ Enable Firewall

☑ Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ, WLAN to WLAN, and VPN to VPN packets will bypass the Firewall check.)

| From \ To | LAN | WAN | DMZ | WLAN | VPN |
|---|---|---|---|---|---|
| LAN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |
| WAN | 2 Rules<br>Drop ☑ | 1 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| DMZ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| WLAN | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| VPN | 0 Rules<br>Drop ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |

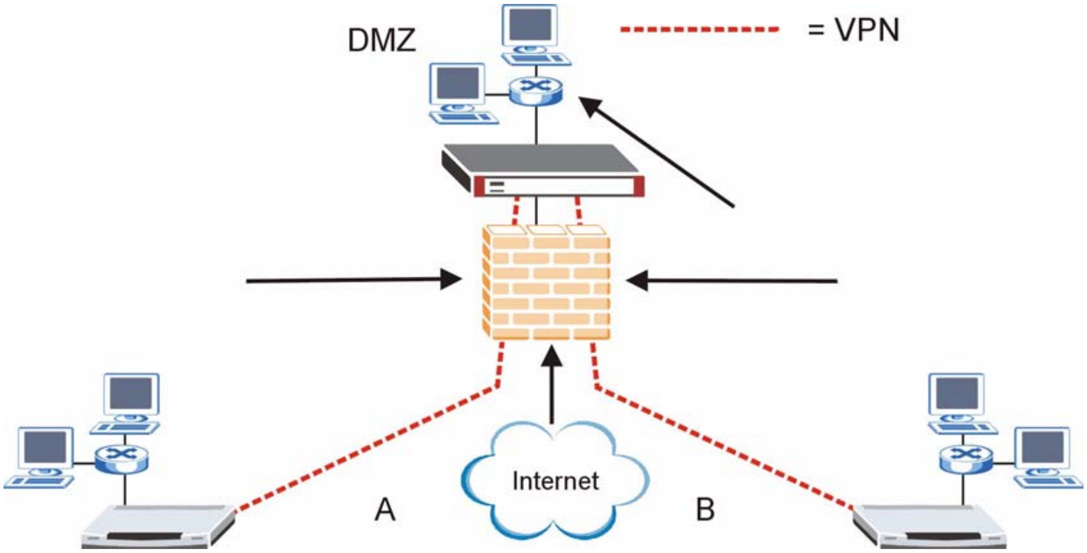
* ☑ Log

### 11.3.3 From VPN To VPN Packet Direction

**From VPN To VPN** firewall rules apply to traffic that comes in through one of the ZyWALL's VPN tunnels and terminates at the ZyWALL (like for remote management) or goes out through another of the ZyWALL's VPN tunnels (this is called hub-and-spoke VPN, see Section 14.17 on page 292 for details). The ZyWALL decrypts the traffic and applies the firewall rules before re-encrypting it or allowing the traffic to terminate at the ZyWALL.

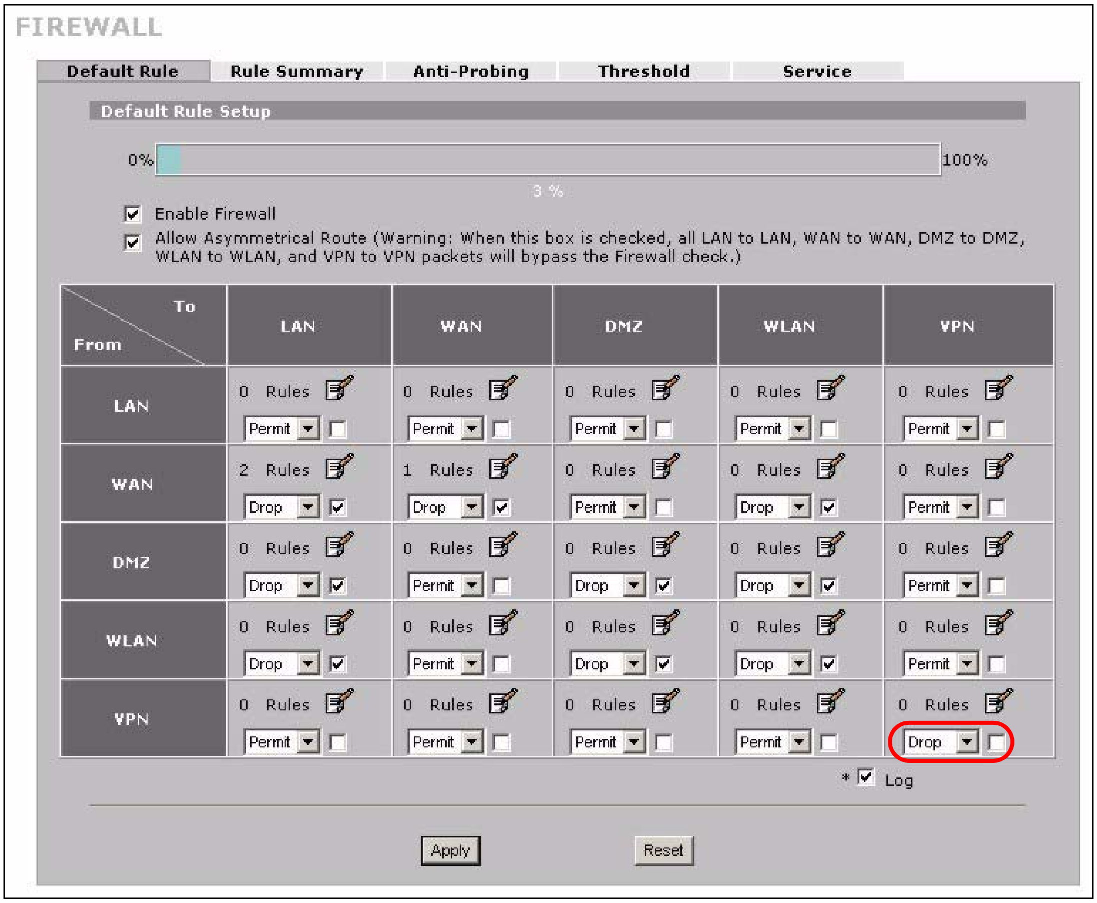
In the following example, the **From VPN To VPN** default firewall rule silently blocks the traffic that the ZyWALL receives from any VPN tunnel (either A or B) that is destined for the other VPN tunnel or the ZyWALL itself. VPN traffic destined for the DMZ is allowed through.

**Figure 130** From VPN to VPN Example



You would configure the **SECURITY** > **FIREWALL** > **Default Rule** screen as follows.

**Figure 131** Block VPN to VPN Traffic by Default Example



☑ Enable Firewall

☑ Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ, WLAN to WLAN, and VPN to VPN packets will bypass the Firewall check.)

| From \ To | LAN | WAN | DMZ | WLAN | VPN |
|---|---|---|---|---|---|
| LAN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |
| WAN | 2 Rules<br>Drop ☑ | 1 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| DMZ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| WLAN | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| VPN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☐ |

* ☑ Log

## 11.4 Security Considerations

Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyWALL and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

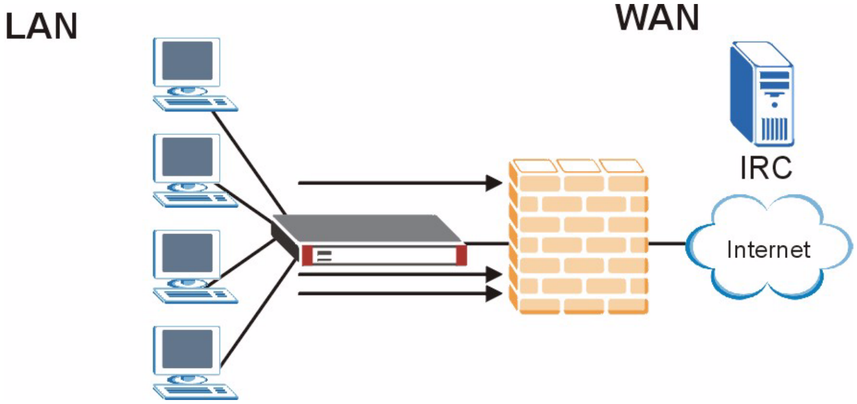
1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

## 11.5 Firewall Rules Example

Suppose that your company decides to block all of the LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN firewall rule that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the firewall rule to always be in effect. The following figure shows the results of this rule.

**Figure 132** Blocking All LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

**Table 46** Blocking All LAN to WAN IRC Traffic Example

| # | SOURCE | DESTINATION | SCHEDULE | SERVICE | ACTION |
|---|---|---|---|---|---|
| 1 | Any | Any | Any | IRC | Drop |
| Default | Any | Any | Any | Any | Allow |

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the firewall’s default policy that allows all traffic from the LAN to go to the WAN.

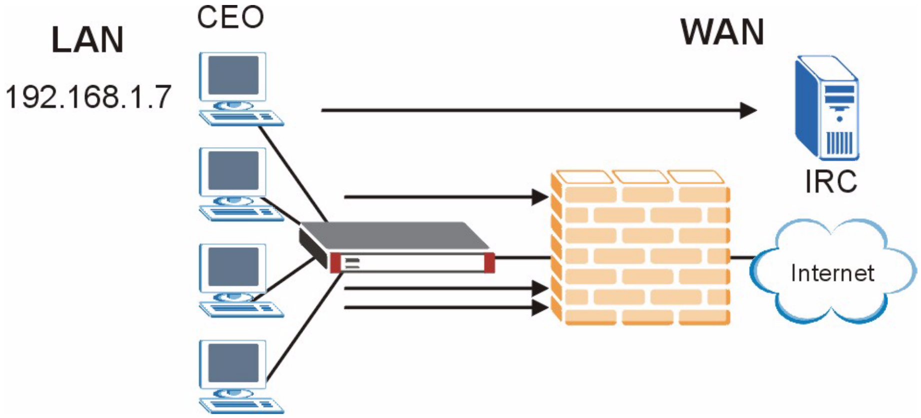
The ZyWALL applies the firewall rules in order. So for this example, when the ZyWALL receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the default rule and the ZyWALL forwards it.

Now suppose that your company wants to let the CEO use IRC. You can configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO’s computer. In order to make sure that the CEO’s computer always uses the same IP address, make sure it either:

- has a static IP address,
- or you configure a static DHCP entry for it so the ZyWALL always assigns it the same IP address (see Section 6.8 on page 139 for information on static DHCP).

Now you configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer (192.168.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the firewall rule to always be in effect. The following figure shows the results of your two custom rules.

**Figure 133** Limited LAN to WAN IRC Traffic Example



Your firewall would have the following configuration.

**Table 47** Limited LAN to WAN IRC Traffic Example

| # | SOURCE | DESTINATIO N | SCHEDULE | SERVICE | ACTION |
|---|---|---|---|---|---|
| 1 | 192.168.1.7 | Any | Any | IRC | Allow |
| 2 | Any | Any | Any | IRC | Drop |
| Default | Any | Any | Any | Any | Allow |

- The first row allows the LAN computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN access to the IRC service on the WAN.
- The third row is (still) the firewall's default policy of allowing all traffic from the LAN to go to the WAN.

The rule for the CEO must come before the rule that blocks all LAN to WAN IRC traffic. If the rule that blocks all LAN to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the ZyWALL would drop it and not check any other firewall rules.

## 11.6 Asymmetrical Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged.

You can have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection).

Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use IP alias to put the ZyWALL and the backup gateway on separate subnets.

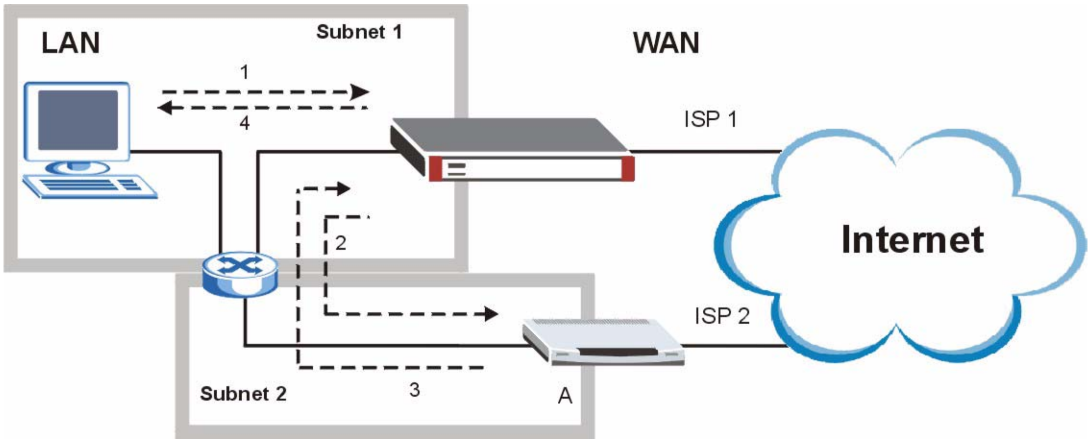
### 11.6.1 Asymmetrical Routes and IP Alias

You can use IP alias instead of allowing asymmetrical routes. IP Alias allow you to partition your network into logical sections over the same interface.

By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the ZyWALL to your LAN. The following steps describe such a scenario.

1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The ZyWALL reroutes the packet to Gateway **A**, which is in **Subnet 2**.
3. The reply from the WAN goes to the ZyWALL.
4. The ZyWALL then sends it to the computer on the LAN in **Subnet 1**.

**Figure 134** Using IP Alias to Solve the Triangle Route Problem

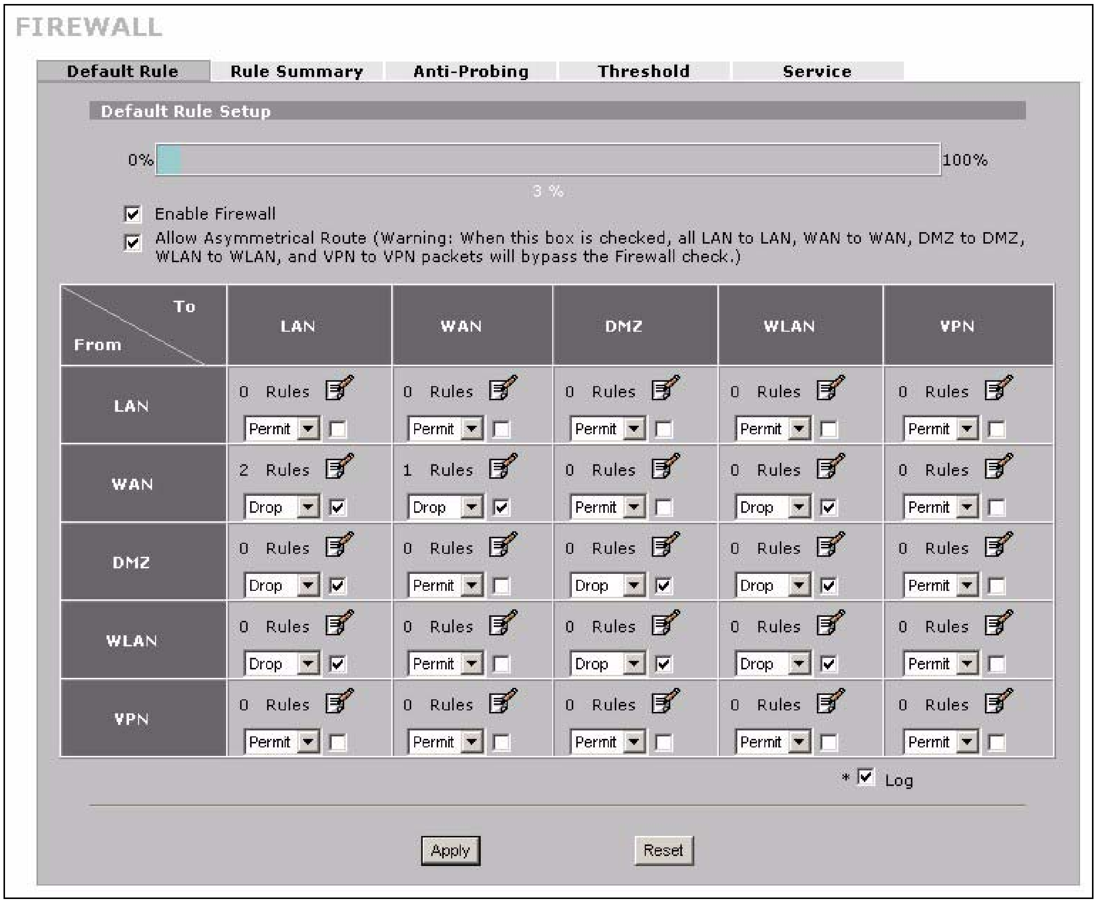


## 11.7 Firewall Default Rule (Router Mode)

Click **SECURITY** > **FIREWALL** to open the **Default Rule** screen.

Use this screen to configure general firewall settings when the ZyWALL is set to router mode.

**Figure 135** SECURITY > FIREWALL > Default Rule (Router Mode)



☑ Enable Firewall

☑ Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ, WLAN to WLAN, and VPN to VPN packets will bypass the Firewall check.)

| From \ To | LAN | WAN | DMZ | WLAN | VPN |
|---|---|---|---|---|---|
| LAN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |
| WAN | 2 Rules<br>Drop ☑ | 1 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| DMZ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| WLAN | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ | 0 Rules<br>Drop ☑ | 0 Rules<br>Drop ☑ | 0 Rules<br>Permit ☐ |
| VPN | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ | 0 Rules<br>Permit ☐ |

* ☑ Log

The following table describes the labels in this screen.

**Table 48** SECURITY > FIREWALL > Default Rule (Router Mode)

| LABEL | DESCRIPTION |
|---|---|
| 0-100% | This bar displays the percentage of the ZyWALL’s firewall rules storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary firewall rules before adding more firewall rules. |
| Enable Firewall | Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.<br>Note: When you activate the firewall, all current connections through the ZyWALL are dropped when you apply your changes. |
| Allow Asymmetrical Route | If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL’s LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or “triangle” route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged.<br>Select this check box to have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection).<br>Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use IP alias to put the ZyWALL and the backup gateway on separate subnets. See Section 11.6.1 on page 202 for an example. |

**Table 48** SECURITY > FIREWALL > Default Rule (Router Mode) (continued)

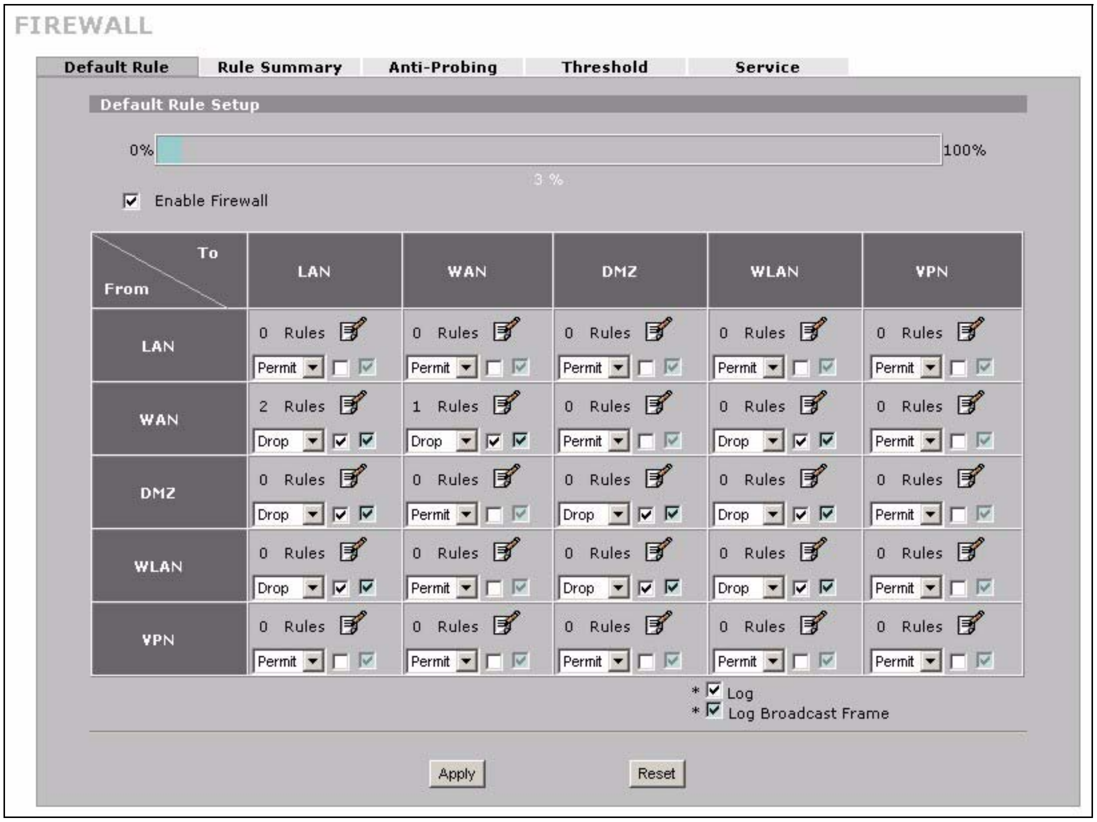
| LABEL | DESCRIPTION |
|---|---|
| From, To | The firewall rules are grouped by the direction of packet travel. This displays the number of rules for each packet direction. Click the edit icon to go to a summary screen of the rules for that packet direction.<br>Here are some example descriptions of the directions of travel.<br>**From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the ZyWALL or the ZyWALL itself. The ZyWALL does not apply the firewall to packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN. The ZyWALL applies the firewall to the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL applies the firewall to the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the ZyWALL. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the ZyWALL. The ZyWALL applies the firewall to the traffic after decrypting it.<br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).<br>Use the drop-down list box to set the firewall's default actions based on the direction of travel of packets.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets.<br>The firewall rules for the WAN port with a higher route priority also apply to the dial backup connection. |
| Log | Select the check box next to a direction of packet travel to create a log when the above action is taken for packets that are traveling in that direction and do not match any of your customized rules. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 11.8 Firewall Default Rule (Bridge Mode)

Click **SECURITY** > **FIREWALL** to open the **Default Rule** screen.

Use this screen to configure general firewall settings when the ZyWALL is set to bridge mode. See Section 11.1 on page 191 for more information about the firewall.

**Figure 136** SECURITY > FIREWALL > Default Rule (Bridge Mode)



☑ Enable Firewall

| To / From | LAN | WAN | DMZ | WLAN | VPN |
|---|---|---|---|---|---|
| LAN | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Permit ☐ ☑ |
| WAN | 2 Rules<br>Drop ☑ ☑ | 1 Rules<br>Drop ☑ ☑ | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Drop ☑ ☑ | 0 Rules<br>Permit ☐ ☑ |
| DMZ | 0 Rules<br>Drop ☑ ☑ | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Drop ☑ ☑ | 0 Rules<br>Drop ☑ ☑ | 0 Rules<br>Permit ☐ ☑ |
| WLAN | 0 Rules<br>Drop ☑ ☑ | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Drop ☑ ☑ | 0 Rules<br>Drop ☑ ☑ | 0 Rules<br>Permit ☐ ☑ |
| VPN | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Permit ☐ ☑ | 0 Rules<br>Permit ☐ ☑ |

* ☑ Log
* ☑ Log Broadcast Frame

The following table describes the labels in this screen.

**Table 49** SECURITY > FIREWALL > Default Rule (Bridge Mode)

| LABEL | DESCRIPTION |
|---|---|
| 0-100% | This bar displays the percentage of the ZyWALL's firewall rules storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary firewall rules before adding more firewall rules. |
| Enable Firewall | Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.<br>Note: When you activate the firewall, all current connections through the ZyWALL are dropped when you apply your changes. |

**Table 49** SECURITY > FIREWALL > Default Rule (Bridge Mode)

| LABEL | DESCRIPTION |
|---|---|
| From, To | The firewall rules are grouped by the direction of packet travel. This displays the number of rules for each packet direction. Click the edit icon to go to a summary screen of the rules for that packet direction.<br>Here are some example descriptions of the directions of travel.<br>**From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the ZyWALL or the ZyWALL itself. The ZyWALL does not apply the firewall to packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected “to” interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN. The ZyWALL applies the firewall to the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected “from” interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL applies the firewall to the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the ZyWALL. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the ZyWALL. The ZyWALL applies the firewall to the traffic after decrypting it.<br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL’s VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).<br>Use the drop-down list box to set the firewall’s default actions based on the direction of travel of packets.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets.<br>The firewall rules for the WAN port with a higher route priority also apply to the dial backup connection. |
| Log | Select this to create a log when the above action is taken. |
| Log Broadcast Frame | Select this to create a log for any broadcast frames traveling in the selected direction. Many of these logs in a short time period could indicate a broadcast storm. A broadcast storm occurs when a packet triggers multiple responses from all hosts on a network or when computers attempt to respond to a host that never replies. As a result, duplicated packets are continuously created and circulated in the network, thus reducing network performance or even rendering it inoperable. A broadcast storm can be caused by an attack on the network, an incorrect network topology (such as a bridge loop) or a malfunctioning network device. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 11.9 Firewall Rule Summary

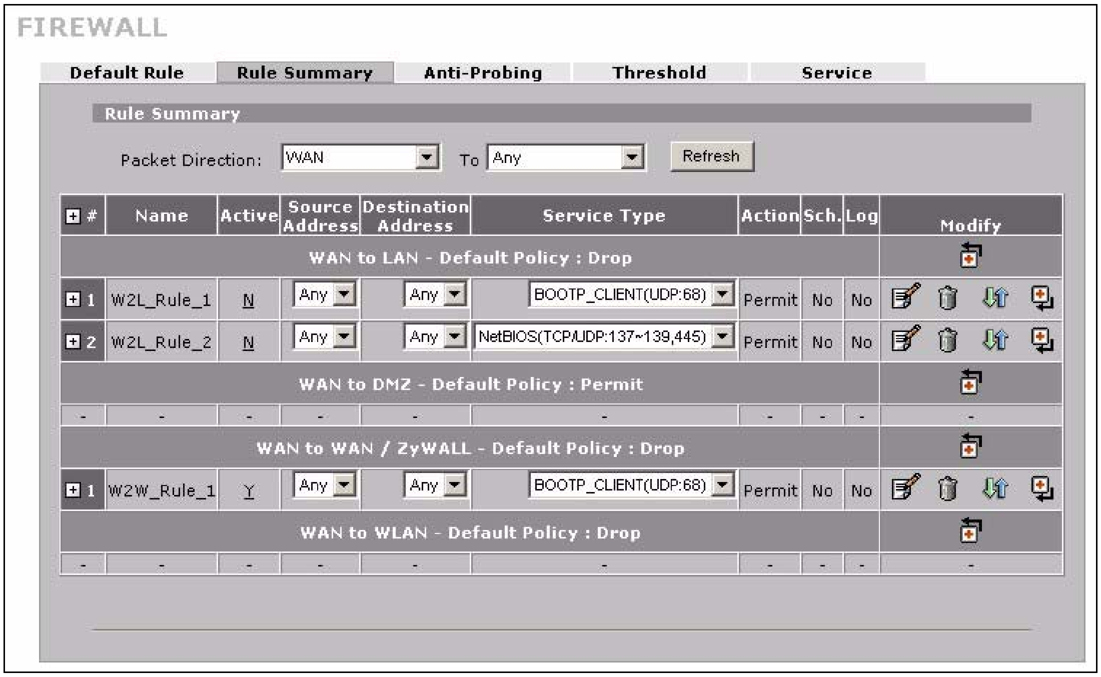
Click **SECURITY** > **FIREWALL** > **Rule Summary** to open the screen. This screen displays a list of the configured firewall rules.

The ordering of your rules is very important as rules are applied in the order that they are listed.

See Section 11.1 on page 191 for more information about the firewall.

- When the ZyWALL is in bridge mode, enable the default **WAN to LAN** firewall rule for the **BOOTP_CLIENT** service to let DHCP clients behind the ZyWALL use a DHCP server on the WAN.
- Enable the default **WAN to LAN** firewall rule for the **NetBIOS** service to let computers behind the ZyWALL access devices on the WAN using computer names.

**Figure 137** SECURITY > FIREWALL > Rule Summary



Packet Direction: WAN To Any

| + # | Name | Active | Source Address | Destination Address | Service Type | Action | Sch. | Log | Modify |
|---|---|---|---|---|---|---|---|---|---|
| WAN to LAN - Default Policy : Drop | | | | | | | | | |
| + 1 | W2L_Rule_1 | N | Any | Any | BOOTP_CLIENT(UDP:68) | Permit | No | No | |
| + 2 | W2L_Rule_2 | N | Any | Any | NetBIOS(TCP/UDP:137~139,445) | Permit | No | No | |
| WAN to DMZ - Default Policy : Permit | | | | | | | | | |
| - | - | - | - | - | - | - | - | - | - |
| WAN to WAN / ZyWALL - Default Policy : Drop | | | | | | | | | |
| + 1 | W2W_Rule_1 | Y | Any | Any | BOOTP_CLIENT(UDP:68) | Permit | No | No | |
| WAN to WLAN - Default Policy : Drop | | | | | | | | | |
| - | - | - | - | - | - | - | - | - | - |

The following table describes the labels in this screen.

**Table 50** SECURITY > FIREWALL > Rule Summary

| LABEL | DESCRIPTION |
|---|---|
| Packet Direction | Use the drop-down list boxes and click **Refresh** to select a direction of travel of packets for which you want to display firewall rules.<br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). |
| +/- | In the heading row, click + to expand or - to collapse the **Source Address**, **Destination Address** and **Service Type** drop down lists for all of the displayed rules. |
| Default Policy | This field displays the default action you selected in the **Default Rule** screen for the packet direction displayed. |

**Table 50** SECURITY > FIREWALL > Rule Summary

| LABEL | DESCRIPTION |
|---|---|
| The following fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above. | |
| # | This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click + to expand or - to collapse the **Source Address**, **Destination Address** and **Service Type** drop down lists. |
| Name | This is the name of the firewall rule. |
| Active | This field displays whether a firewall is turned on (**Y**) or not (**N**). Click the setting to change it. |
| Source Address | This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**. |
| Destination Address | This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**. |
| Service Type | This drop-down list box displays the services to which this firewall rule applies. Custom services have an * before the name. See Appendix D on page 653 for a list of common services. |
| Action | This field displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**) or allows the passage of packets (**Permit**). |
| Sch. | This field tells you whether a schedule is specified (**Yes**) or not (**No**). |
| Log | This field shows you whether a log is created when packets match this rule (**Yes**) or not (**No**). |
| Modify | Click the edit icon to go to the screen where you can edit the rule.<br>Click the delete icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.<br>Click the insert icon to display the screen where you can configure a new firewall rule. The insert icon at the top of the row creates the new firewall rule before the others. The individual firewall rule insert icons create a new firewall rule after the row's firewall rule.<br>Click the move icon, type an index number, and press Enter to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering. |

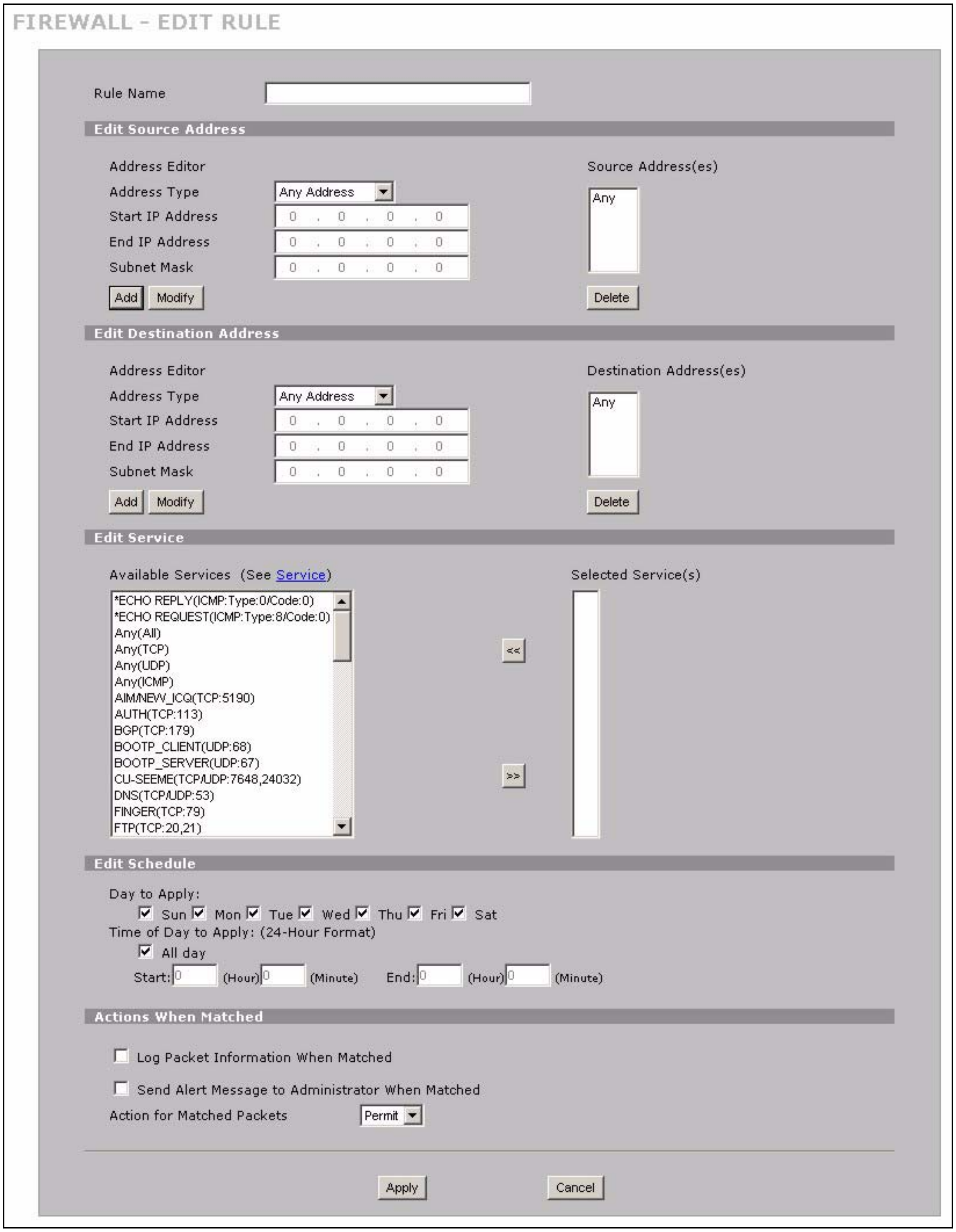
## 11.9.1 Firewall Edit Rule

In the **Rule Summary** screen, click the edit icon or the insert icon to display the **Firewall Edit Rule** screen.

Use this screen to create or edit a firewall rule. Refer to the following table for information on the labels.

See Section 11.1 on page 191 for more information about the firewall.

**Figure 138** SECURITY > FIREWALL > Rule Summary > Edit



FIREWALL - EDIT RULE

Rule Name

Edit Source Address

Address Editor
Address Type: Any Address
Start IP Address: 0 . 0 . 0 . 0
End IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Source Address(es): Any

Edit Destination Address

Address Editor
Address Type: Any Address
Start IP Address: 0 . 0 . 0 . 0
End IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Destination Address(es): Any

Edit Service

Available Services (See Service)
*ECHO REPLY(ICMP:Type:0/Code:0)
*ECHO REQUEST(ICMP:Type:8/Code:0)
Any(All)
Any(TCP)
Any(UDP)
Any(ICMP)
AIM/NEW_ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)
BOOTP_CLIENT(UDP:68)
BOOTP_SERVER(UDP:67)
CU-SEEME(TCP/UDP:7648,24032)
DNS(TCP/UDP:53)
FINGER(TCP:79)
FTP(TCP:20,21)

Selected Service(s)

Edit Schedule

Day to Apply:
☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat
Time of Day to Apply: (24-Hour Format)
☑ All day
Start: 0 (Hour) 0 (Minute) End: 0 (Hour) 0 (Minute)

Actions When Matched

☐ Log Packet Information When Matched
☐ Send Alert Message to Administrator When Matched
Action for Matched Packets: Permit

The following table describes the labels in this screen.

**Table 51** SECURITY > FIREWALL > Rule Summary > Edit

| LABEL | DESCRIPTION |
|---|---|
| Rule Name | Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the firewall rule. Spaces are allowed. |
| Edit Source/ Destination Address | |
| Address Type | Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**. |
| Start IP Address | Enter the single IP address or the starting IP address in a range here. |
| End IP Address | Enter the ending IP address in a range here. |
| Subnet Mask | Enter the subnet mask here, if applicable. |
| Add | Click **Add** to add a new address to the **Source** or **Destination Address(es)** box. You can add multiple addresses, ranges of addresses, and/or subnets. |
| Modify | To edit an existing source or destination address, select it from the box and click **Modify**. |
| Delete | Highlight an existing source or destination address from the **Source** or **Destination Address(es)** box above and click **Delete** to remove it. |
| Edit Service | |
| Available/ Selected Services | Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Service(s)** box on the right. To remove a service, highlight it in the **Selected Service(s)** box on the right, then click **<<**.<br>Next to the name of a service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type). For example, look at the DNS entry, (UDP/TCP:53) means UDP port 53 and TCP port 53. Click the **Service** link to go to the **Service** screen where you can configure custom service ports. See Appendix D on page 653 for a list of commonly used services and port numbers.<br>You can use the [CTRL] key and select multiple services at once. |
| Edit Schedule | |
| Day to Apply | Select everyday or the day(s) of the week to apply the rule. |
| Time of Day to Apply (24-Hour Format) | Select **All Day** or enter the start and end times in the hour-minute format to apply the rule. |
| Actions When Matched | |
| Log Packet Information When Matched | This field determines if a log for packets that match the rule is created (**Yes**) or not (**No**). Go to the **Log Settings** page and select the **Access Control** logs category to have the ZyWALL record these logs. |
| Send Alert Message to Administrator When Matched | Select the check box to have the ZyWALL generate an alert when the rule is matched. |

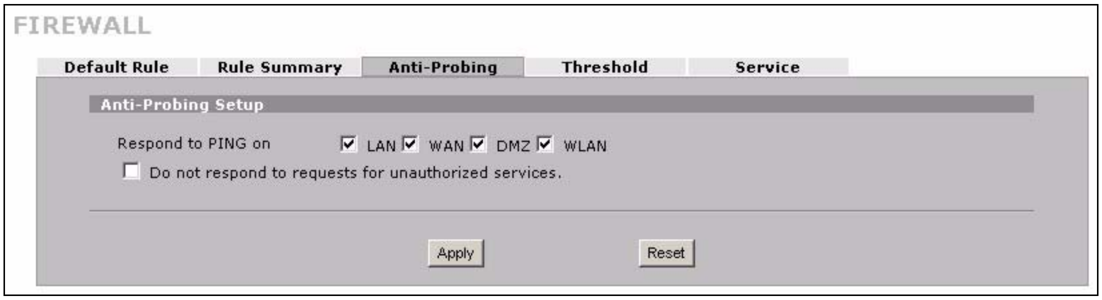
**Table 51** SECURITY > FIREWALL > Rule Summary > Edit

| LABEL | DESCRIPTION |
|---|---|
| Action for Matched Packets | Use the drop-down list box to select what the firewall is to do with packets that match this rule.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets.<br>Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) if you want to allow computers on the WAN to access devices on the LAN.<br>Note: You may also need to configure the remote management settings if you want to allow a WAN computer to manage the ZyWALL or restrict management from the LAN. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 11.10 Anti-Probing

Click **SECURITY** > **FIREWALL** > **Anti-Probing** to open the following screen. Configure this screen to help keep the ZyWALL hidden from probing attempts. You can specify which of the ZyWALL's interfaces will respond to Ping requests and whether or not the ZyWALL is to respond to probing for unused ports.

**Figure 139** SECURITY > FIREWALL > Anti-Probing



Respond to PING on ☑ LAN ☑ WAN ☑ DMZ ☑ WLAN

☐ Do not respond to requests for unauthorized services.

The following table describes the labels in this screen.

**Table 52** SECURITY > FIREWALL > Anti-Probing

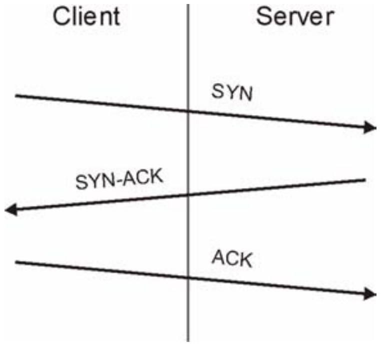
| LABEL | DESCRIPTION |
|---|---|
| Respond to PING on | Select the check boxes of the interfaces that you want to reply to incoming Ping requests.<br>Clear an interface's check box to have the ZyWALL not respond to any Ping requests that come into that interface. |
| Do not respond to requests for unauthorized services. | Select this option to prevent hackers from finding the ZyWALL by probing for unused ports. If you select this option, the ZyWALL will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyWALL unseen. If this option is not selected, the ZyWALL will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports.<br>Note that the probing packets must first traverse the ZyWALL's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the ZyWALL reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 11.11 Firewall Thresholds

For DoS attacks, the ZyWALL uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions.

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

**Figure 140** Three-Way Handshake



For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

### 11.11.1 Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the ZyWALL has been receiving DoS attacks that are not recorded in the logs or the logs show that the ZyWALL is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

1. The maximum number of opened sessions.
2. The minimum capacity of server backlog in your LAN network.
3. The CPU power of servers in your LAN network.
4. Network bandwidth.
5. Type of traffic for certain servers.

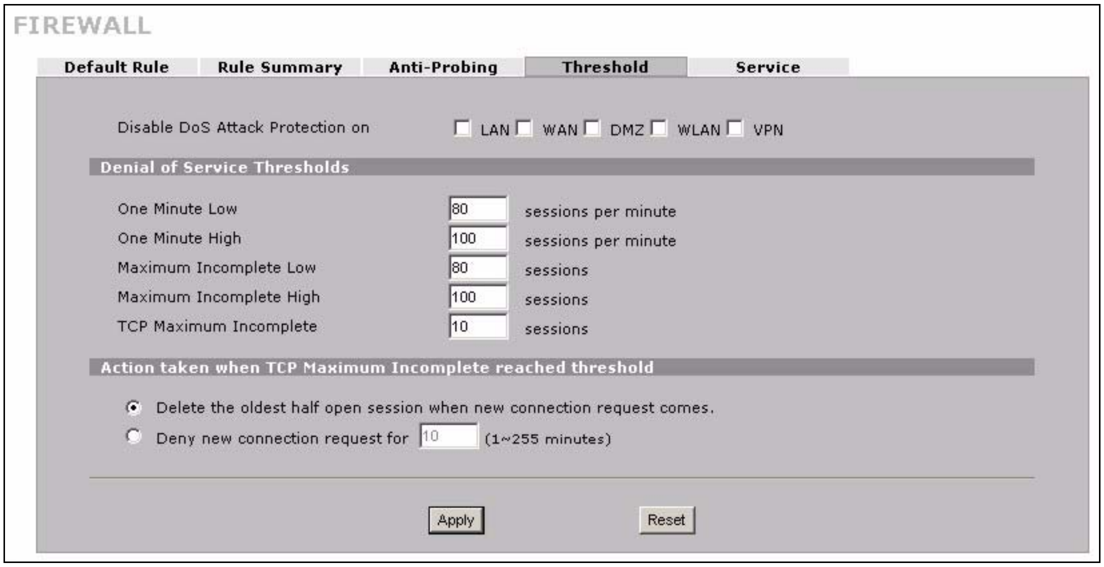
Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the ZyWALL may classify them as DoS attacks.

## 11.12 Threshold Screen

Click **SECURITY** > **FIREWALL** > **Threshold** to bring up the next screen. The global values specified for the threshold and timeout apply to all TCP connections.

**Figure 141** SECURITY > FIREWALL > Threshold



Disable DoS Attack Protection on ☐ LAN ☐ WAN ☐ DMZ ☐ WLAN ☐ VPN

Denial of Service Thresholds

One Minute Low 80 sessions per minute
One Minute High 100 sessions per minute
Maximum Incomplete Low 80 sessions
Maximum Incomplete High 100 sessions
TCP Maximum Incomplete 10 sessions

Action taken when TCP Maximum Incomplete reached threshold

● Delete the oldest half open session when new connection request comes.
○ Deny new connection request for 10 (1~255 minutes)

The following table describes the labels in this screen.

**Table 53** SECURITY > FIREWALL > Threshold

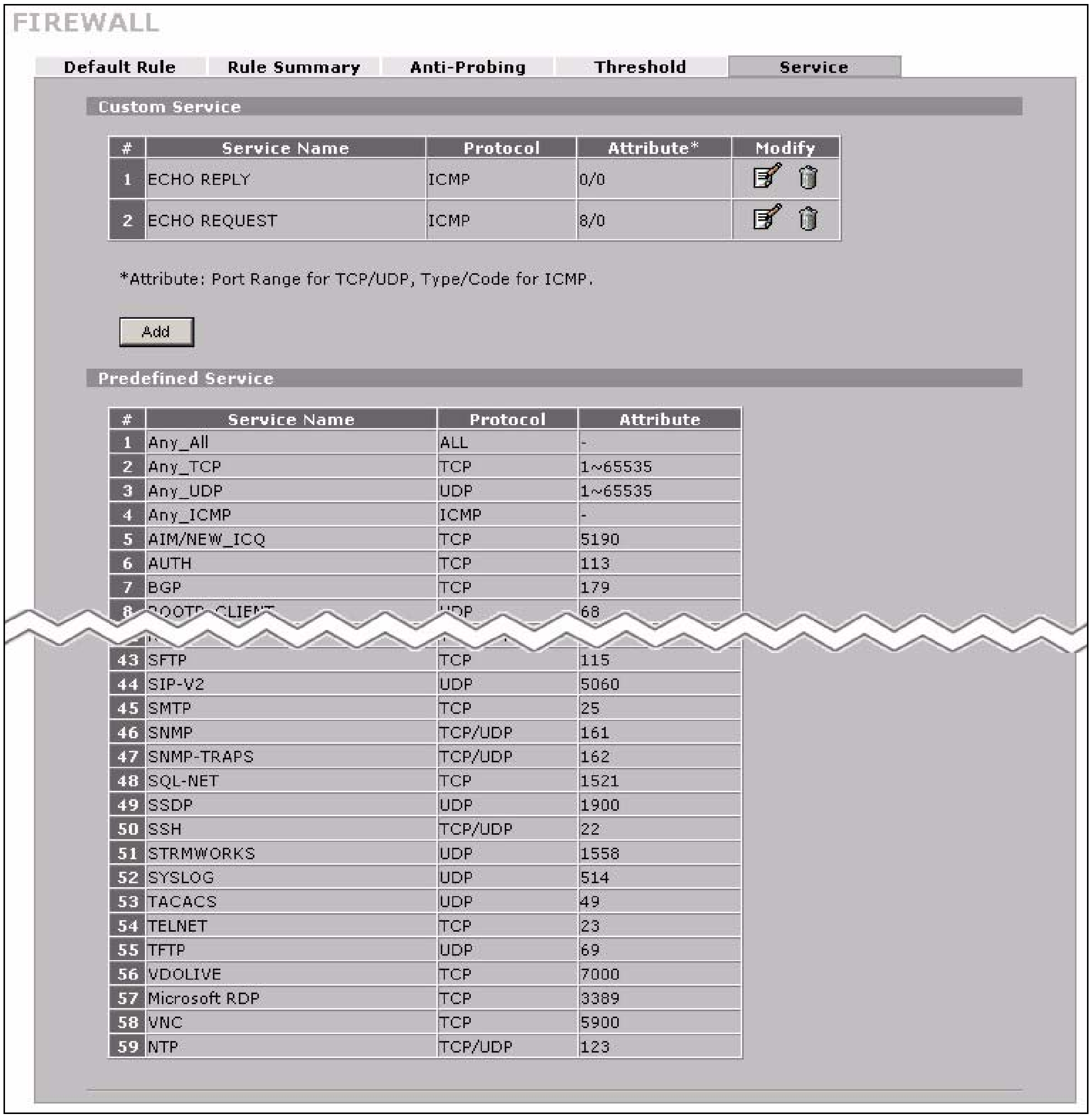
| LABEL | DESCRIPTION |
|---|---|
| Disable DoS Attack Protection on | Select the check boxes of any interfaces (or all VPN tunnels) for which you want the ZyWALL to not use the Denial of Service protection thresholds. This disables DoS protection on the selected interface (or all VPN tunnels).<br>You may want to disable DoS protection for an interface if the ZyWALL is treating valid traffic as DoS attacks. Another option would be to raise the thresholds. |
| Denial of Service Thresholds | The ZyWALL measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute. |
| One Minute Low | This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number. |
| One Minute High | This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection attempts.<br>For example, if you set the one minute high to 100, the ZyWALL starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low. |
| Maximum Incomplete Low | This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number. |
| Maximum Incomplete High | This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number.<br>For example, if you set the maximum incomplete high to 100, the ZyWALL starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low. |
| TCP Maximum Incomplete | An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host.<br>Specify the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. The ZyWALL sends alerts whenever the **TCP Maximum Incomplete** is exceeded. |
| Action taken when TCP Maximum Incomplete reached threshold | Select the action that ZyWALL should take when the TCP maximum incomplete threshold is reached. You can have the ZyWALL either:<br>Delete the oldest half open session when a new connection request comes.<br>or<br>Deny new connection requests for the number of minutes that you specify (between 1 and 255). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 11.13 Service

Click **SECURITY** > **FIREWALL** > **Service** to open the screen as shown next. Use this screen to configure custom services for use in firewall rules or view the services that are predefined in the ZyWALL.

See Section 11.1 on page 191 for more information about the firewall.

**Figure 142** SECURITY > FIREWALL > Service



Custom Service

| # | Service Name | Protocol | Attribute* | Modify |
|---|---|---|---|---|
| 1 | ECHO REPLY | ICMP | 0/0 | |
| 2 | ECHO REQUEST | ICMP | 8/0 | |

*Attribute: Port Range for TCP/UDP, Type/Code for ICMP.

Predefined Service

| # | Service Name | Protocol | Attribute |
|---|---|---|---|
| 1 | Any_All | ALL | - |
| 2 | Any_TCP | TCP | 1~65535 |
| 3 | Any_UDP | UDP | 1~65535 |
| 4 | Any_ICMP | ICMP | - |
| 5 | AIM/NEW_ICQ | TCP | 5190 |
| 6 | AUTH | TCP | 113 |
| 7 | BGP | TCP | 179 |
| 8 | BOOTP_CLIENT | UDP | 68 |
| 43 | SFTP | TCP | 115 |
| 44 | SIP-V2 | UDP | 5060 |
| 45 | SMTP | TCP | 25 |
| 46 | SNMP | TCP/UDP | 161 |
| 47 | SNMP-TRAPS | TCP/UDP | 162 |
| 48 | SQL-NET | TCP | 1521 |
| 49 | SSDP | UDP | 1900 |
| 50 | SSH | TCP/UDP | 22 |
| 51 | STRMWORKS | UDP | 1558 |
| 52 | SYSLOG | UDP | 514 |
| 53 | TACACS | UDP | 49 |
| 54 | TELNET | TCP | 23 |
| 55 | TFTP | UDP | 69 |
| 56 | VDOLIVE | TCP | 7000 |
| 57 | Microsoft RDP | TCP | 3389 |
| 58 | VNC | TCP | 5900 |
| 59 | NTP | TCP/UDP | 123 |

The following table describes the labels in this screen.

**Table 54** SECURITY > FIREWALL > Service

| LABEL | DESCRIPTION |
|---|---|
| Custom Service | This table shows all configured custom services. |
| # | This is the index number of the custom service. |
| Service Name | This is the name of the service. |

**Table 54** SECURITY > FIREWALL > Service (continued)

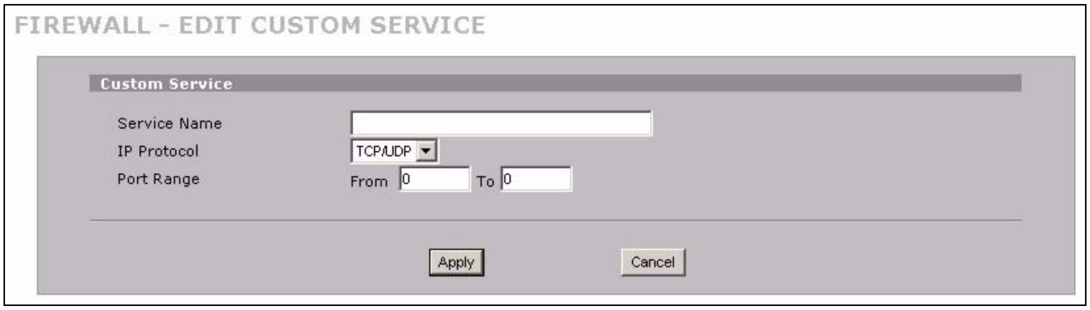
| LABEL | DESCRIPTION |
|---|---|
| Protocol | This is the IP protocol type.<br>If you selected **Custom**, this is the IP protocol value you entered. |
| Attribute | This is the IP port number or ICMP type and code that defines the service. |
| Modify | Click the edit icon to go to the screen where you can edit the service.<br>Click the delete icon to remove an existing service. A window displays asking you to confirm that you want to delete the service. Note that subsequent services move up by one when you take this action. |
| Add | Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services. |
| Predefined Service | This table shows all the services that are already configured for use in firewall rules. See Appendix D on page 653 for a list of common services. |
| # | This is the index number of the predefined service. |
| Service Name | This is the name of the service. |
| Protocol | This is the IP protocol type. There may be more than one IP protocol type. |
| Attribute | This is the IP port number or ICMP type and code that defines the service. |

## 11.13.1 Firewall Edit Custom Service

Click **SECURITY** > **FIREWALL** > **Service** > **Add** to display the following screen. Use this screen to configure a custom service entry not is not predefined in the ZyWALL. See Appendix D on page 653 the user's guide appendices for a list of commonly used services and port numbers.

See Section 11.1 on page 191 for more information about the firewall.

**Figure 143** Firewall Edit Custom Service



Service Name
IP Protocol: TCP/UDP
Port Range: From 0 To 0

The following table describes the labels in this screen.

**Table 55** SECURITY > FIREWALL > Service > Add

| LABEL | DESCRIPTION |
|---|---|
| Service Name | Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the custom service. You cannot use the "(" character. Spaces are allowed. |
| IP Protocol | Choose the IP protocol (**TCP**, **UDP**, **TCP/UDP**, **ICMP** or **Custom**) that defines your customized service from the drop down list box.<br>If you select **Custom**, specify the protocol's number. For example, ICMP is 1, TCP is 6, UDP is 17 and so on. |

**Table 55** SECURITY > FIREWALL > Service > Add (continued)

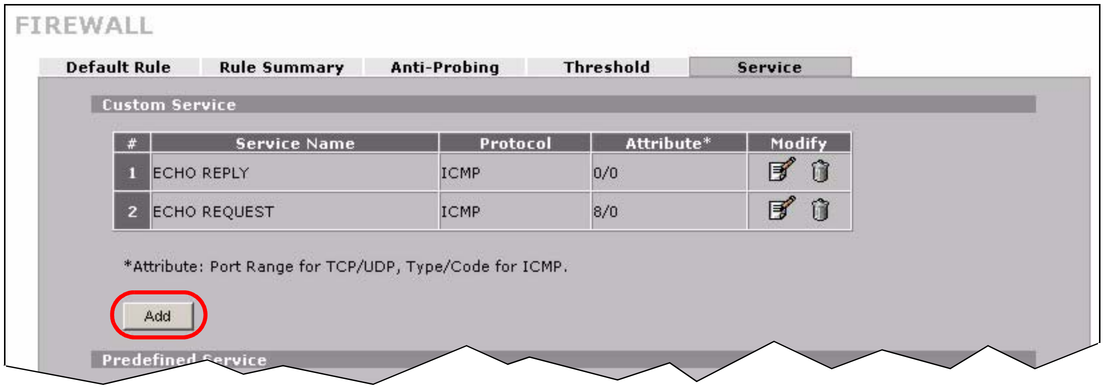
| LABEL | DESCRIPTION |
|---|---|
| Port Range | Enter the port number (from 1 to 255) that defines the customized service<br>To specify one port only, enter the port number in the **From** field and enter it again in the **To** field.<br>To specify a span of ports, enter the first port in the **From** field and enter the last port in the **To** field. |
| Type/Code | This field is available only when you select **ICMP** in the **IP Protocol** field.<br>The ICMP messages are identified by their types and in some cases codes.<br>Enter the type number in the **Type** field and select the **Code** radio button and enter the code number if any. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 11.14 My Service Firewall Rule Example

The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

1 In the **Service** screen, click **Add** to open the **Edit Custom Service** screen.

**Figure 144** My Service Firewall Rule Example: Service

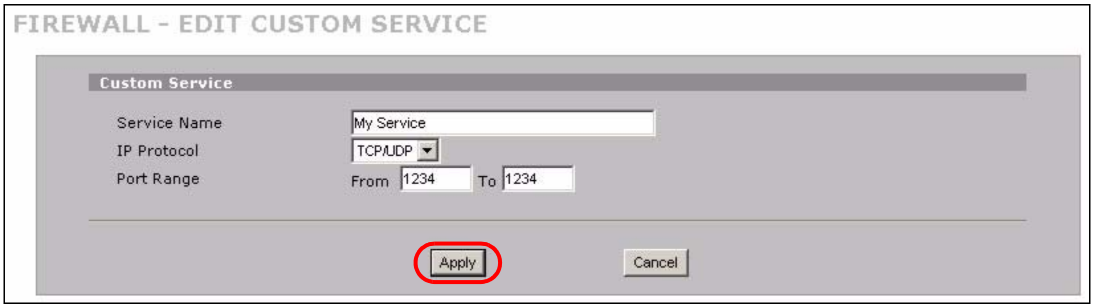


| # | Service Name | Protocol | Attribute* | Modify |
|---|---|---|---|---|
| 1 | ECHO REPLY | ICMP | 0/0 | |
| 2 | ECHO REQUEST | ICMP | 8/0 | |

*Attribute: Port Range for TCP/UDP, Type/Code for ICMP.

2 Configure it as follows and click **Apply**.

**Figure 145** My Service Firewall Rule Example: Edit Custom Service

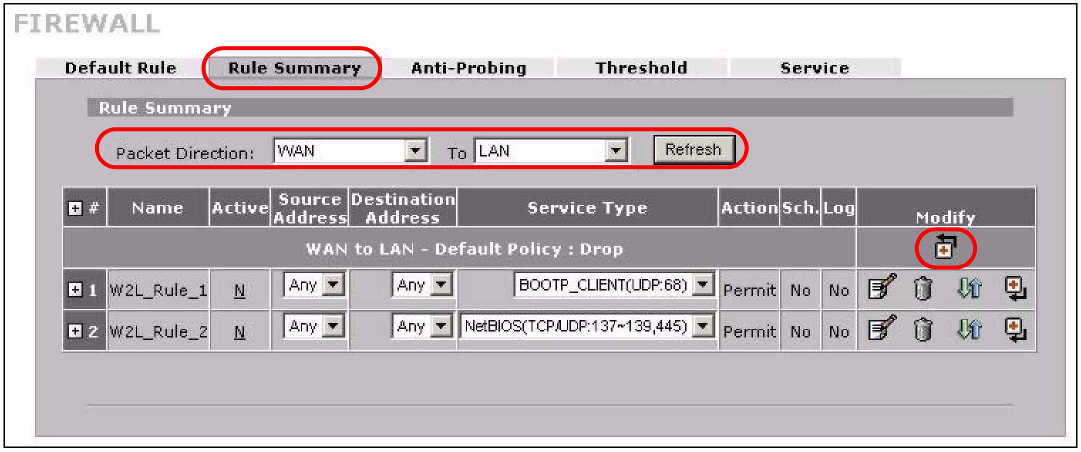


Service Name: My Service
IP Protocol: TCP/UDP
Port Range: From 1234 To 1234

3 Click **Rule Summary**. Select **WAN** and **LAN** from the **Packet Direction** drop-down list boxes and click **Refresh** to display existing firewall rules for the selected direction of travel of packets.

**4** Click the insert icon at the top of the row to create the new firewall rule before the others.

**Figure 146** My Service Firewall Rule Example: Rule Summary


FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Rule Summary
Refresh
Modify

Packet Direction: WAN To LAN

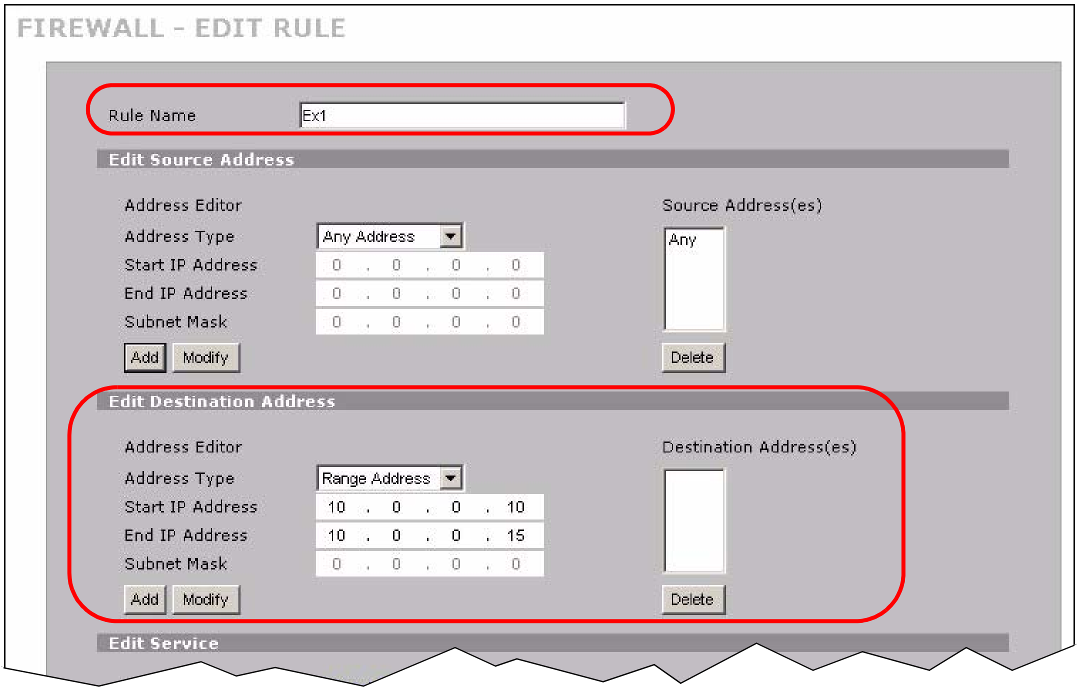
| # | Name | Active | Source Address | Destination Address | Service Type | Action | Sch. | Log |
|---|---|---|---|---|---|---|---|---|
| WAN to LAN - Default Policy : Drop | | | | | | | | |
| 1 | W2L_Rule_1 | N | Any | Any | BOOTP_CLIENT(UDP:68) | Permit | No | No |
| 2 | W2L_Rule_2 | N | Any | Any | NetBIOS(TCP/UDP:137~139,445) | Permit | No | No |

**5** The **Edit Rule** screen displays. Enter the name of the firewall rule.

**6** Select **Any** in the **Destination Address(es)** box and then click **Delete**.

**7** Configure the destination address fields as follows and click **Add**.

**Figure 147** My Service Firewall Rule Example: Rule Edit: Source and Destination Addresses


FIREWALL - EDIT RULE
Edit Source Address
Address Editor
Source Address(es)
Add
Modify
Delete
Edit Destination Address
Address Editor
Destination Address(es)
Add
Modify
Delete
Edit Service

Rule Name: Ex1

Edit Source Address

Address Type: Any Address
Start IP Address: 0 . 0 . 0 . 0
End IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Source Address(es): Any

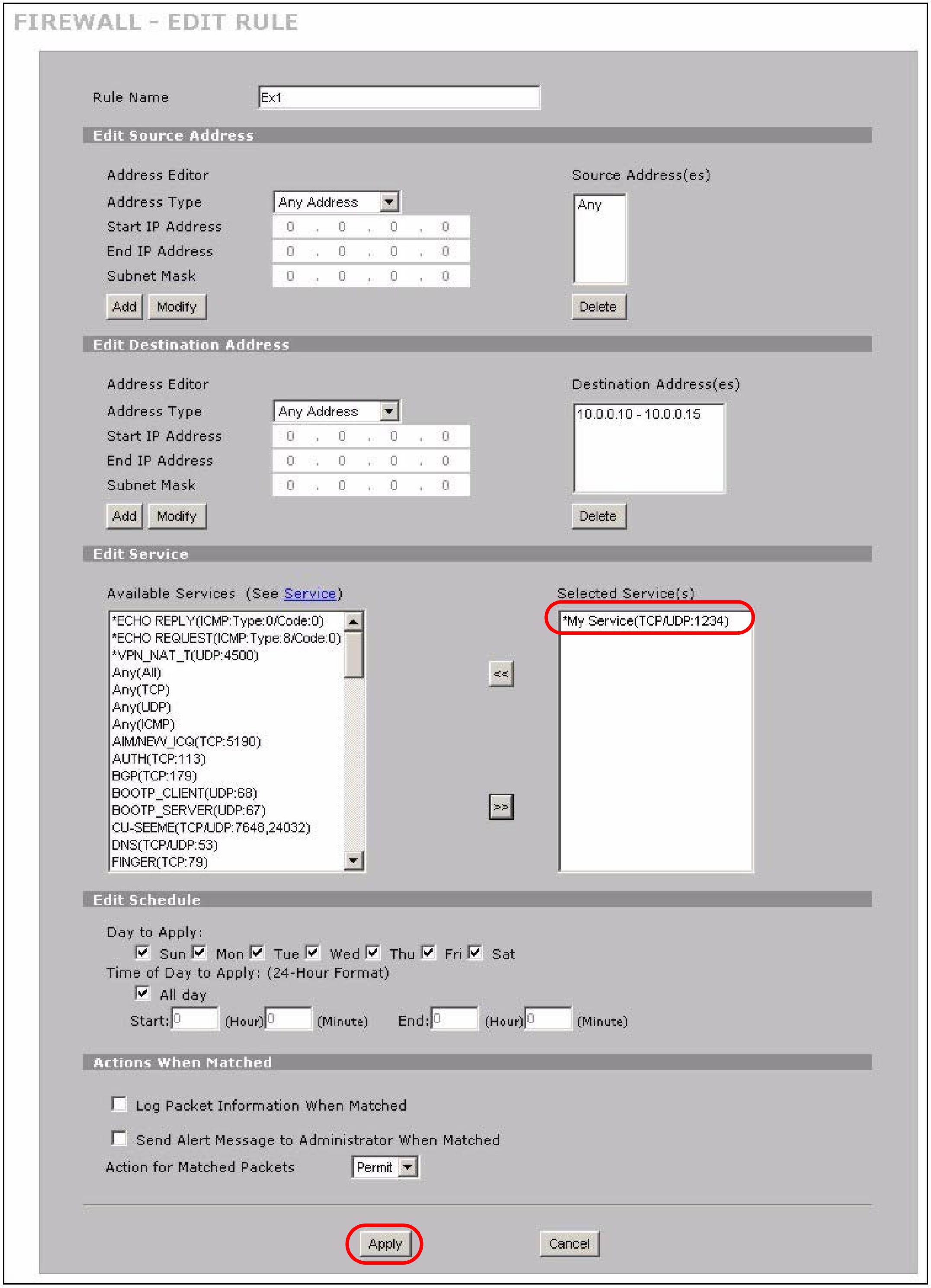
Edit Destination Address

Address Type: Range Address
Start IP Address: 10 . 0 . 0 . 10
End IP Address: 10 . 0 . 0 . 15
Subnet Mask: 0 . 0 . 0 . 0

**8** In the **Edit Service** section, use the arrows between **Available Services** and **Selected Service(s)** to configure it as follows. Click **Apply** when you are done.

Custom services show up with an * before their names in the **Services** list boxes and the **Rule Summary** screen’s **Service Type** list box.

**Figure 148** My Service Firewall Rule Example: Edit Rule: Service Configuration



FIREWALL - EDIT RULE

Rule Name: Ex1

**Edit Source Address**

Address Editor

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Source Address(es): Any

**Edit Destination Address**

Address Editor

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Destination Address(es): 10.0.0.10 - 10.0.0.15

**Edit Service**

Available Services (See Service)

- *ECHO REPLY(ICMP:Type:0/Code:0)
- *ECHO REQUEST(ICMP:Type:8/Code:0)
- *VPN_NAT_T(UDP:4500)
- Any(All)
- Any(TCP)
- Any(UDP)
- Any(ICMP)
- AIM/NEW_ICQ(TCP:5190)
- AUTH(TCP:113)
- BGP(TCP:179)
- BOOTP_CLIENT(UDP:68)
- BOOTP_SERVER(UDP:67)
- CU-SEEME(TCP/UDP:7648,24032)
- DNS(TCP/UDP:53)
- FINGER(TCP:79)

Selected Service(s): *My Service(TCP/UDP:1234)

**Edit Schedule**

Day to Apply:

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Apply: (24-Hour Format)

☑ All day

Start: 0 (Hour) 0 (Minute) End: 0 (Hour) 0 (Minute)

**Actions When Matched**

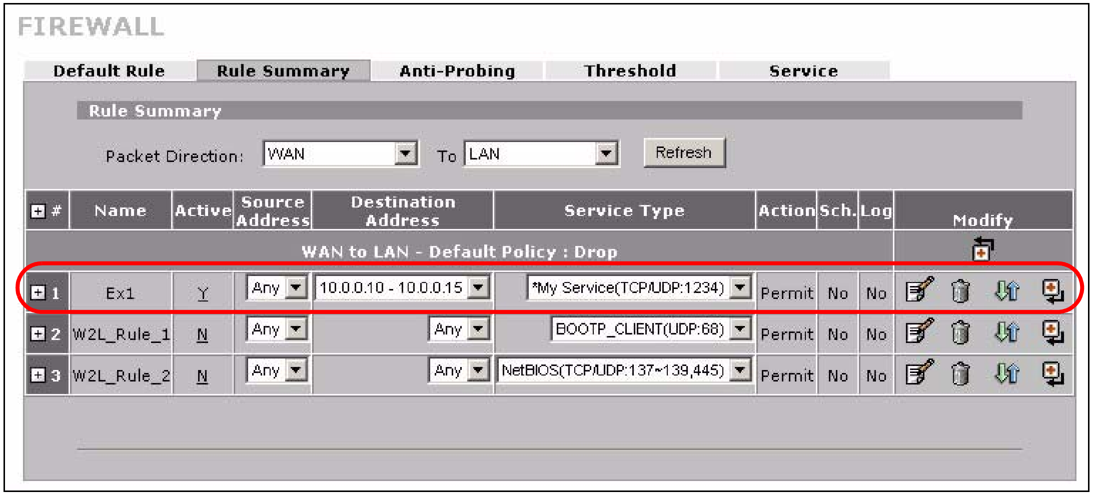
☐ Log Packet Information When Matched

☐ Send Alert Message to Administrator When Matched

Action for Matched Packets: Permit

Rule 1 allows a My Service connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

**Figure 149** My Service Firewall Rule Example: Rule Summary: Completed


FIREWALL
Default Rule
Rule Summary
Anti-Probing
Threshold
Service
Rule Summary
Refresh

Packet Direction: WAN To LAN

| # | Name | Active | Source Address | Destination Address | Service Type | Action | Sch. | Log | Modify |
|---|---|---|---|---|---|---|---|---|---|
| WAN to LAN - Default Policy : Drop | | | | | | | | | |
| 1 | Ex1 | Y | Any | 10.0.0.10 - 10.0.0.15 | *My Service(TCP/UDP:1234) | Permit | No | No | |
| 2 | W2L_Rule_1 | N | Any | Any | BOOTP_CLIENT(UDP:68) | Permit | No | No | |
| 3 | W2L_Rule_2 | N | Any | Any | NetBIOS(TCP/UDP:137~139,445) | Permit | No | No | |

# 12

# Content Filtering Screens

This chapter provides an overview of content filtering.

## 12.1 Content Filtering Overview

Content filtering allows you to block certain web features, such as Cookies, and/or block access to specific websites. With content filtering, you can do the following:

### 12.1.1 Restrict Web Features

The ZyWALL can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

### 12.1.2 Create a Filter List

You can select categories, such as pornography or racial intolerance, to block from a pre-defined list.

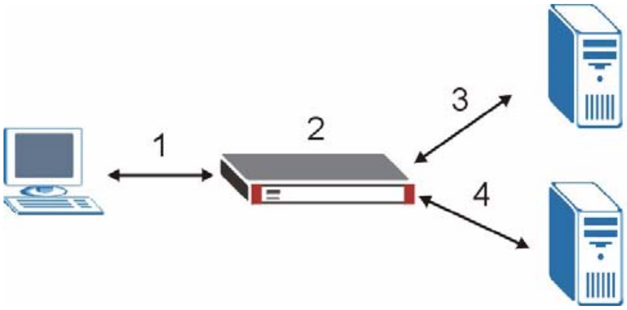
### 12.1.3 Customize Web Site Access

You can specify URLs to which the ZyWALL blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the ZyWALL block access to URLs that contain key words that you specify.

## 12.2 Content Filtering with an External Database

When you register for and enable external database content filtering, your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories. The content filtering lookup process is described below.

**Figure 150** Content Filtering Lookup Procedure



**1** A computer behind the ZyWALL tries to access a web site.

**2** The ZyWALL looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the ZyWALL's cache. The ZyWALL blocks, blocks and logs or just logs the request based on your configuration.

**3** Use the **CONTENT FILTER Cache** screen to configure how long a web site address remains in the cache as well as view those web site addresses (see Section 12.11 on page 243). All of the web site address records are also cleared from the local cache when the ZyWALL restarts.

**4** If the ZyWALL has no record of the web site, it will query the external content filtering database and simultaneously send the request to the web server.

The external content filtering database may change a web site's category or categorize a previously uncategorized web site.

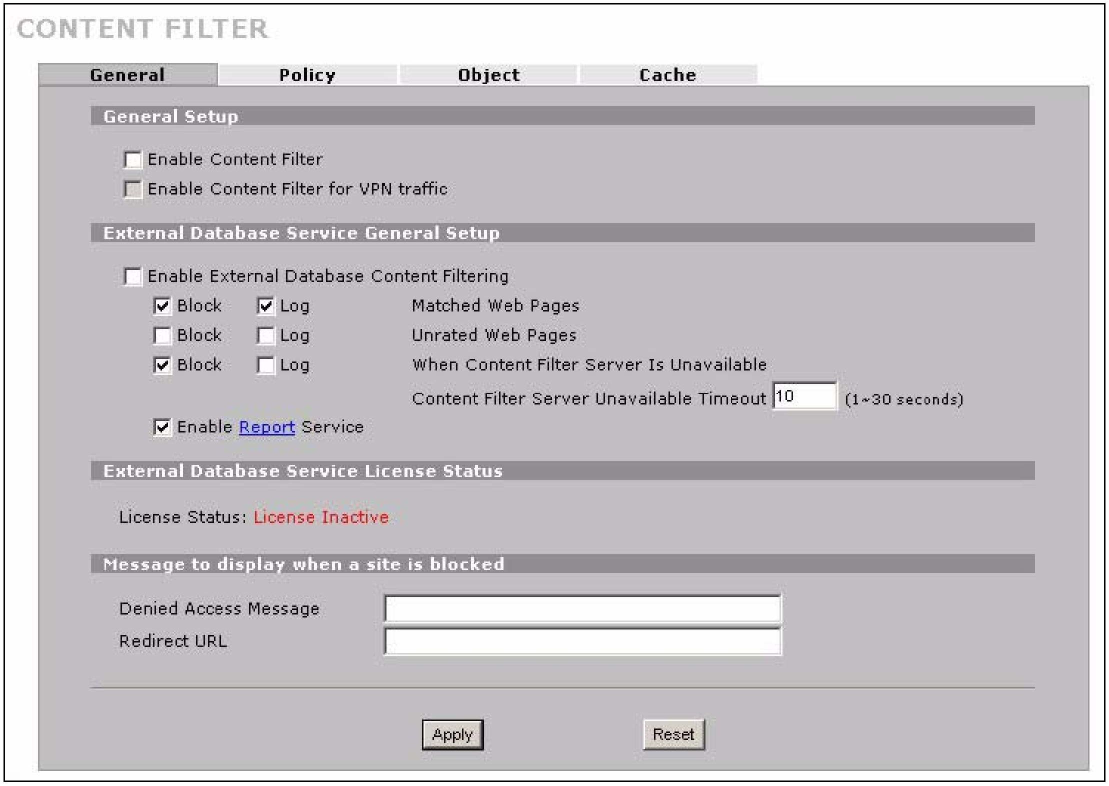
**5** The external content filtering server sends the category information back to the ZyWALL, which then blocks and/or logs access to the web site. The web site's address and category are then stored in the ZyWALL's content filtering cache.

## 12.3 Content Filter General Screen

Click **SECURITY** > **CONTENT FILTER** to open the **CONTENT FILTER General** screen.

Use this screen to enable content filtering and configure general settings. You must register for external content filtering before you can use it. Use the **REGISTRATION** screens (see Chapter 5 on page 127) to create a myZyXEL.com account, register your device and activate the external content filtering service.

**Figure 151** SECURITY > CONTENT FILTER > General



General Setup

☐ Enable Content Filter
☐ Enable Content Filter for VPN traffic

External Database Service General Setup

☐ Enable External Database Content Filtering
☑ Block ☑ Log Matched Web Pages
☐ Block ☐ Log Unrated Web Pages
☑ Block ☐ Log When Content Filter Server Is Unavailable
Content Filter Server Unavailable Timeout 10 (1~30 seconds)
☑ Enable Report Service

External Database Service License Status

License Status: License Inactive

Message to display when a site is blocked

Denied Access Message
Redirect URL

The following table describes the labels in this screen.

**Table 56** SECURITY > CONTENT FILTER > General

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Content Filter | Select this check box to enable the content filter. Content filtering works on HTTP traffic that is using TCP ports 80, 119, 3128 or 8080.<br>See Section 23.1 on page 409 if you need to use content filtering for traffic on custom ports. |
| Enable Content Filter for VPN traffic | Select this check box to have the content filter apply to traffic that the ZyWALL sends out through a VPN tunnel or receives through a VPN tunnel. The ZyWALL applies the content filter to the traffic before encrypting it or after decrypting it.<br>Note: The ZyWALL can apply content filtering on the traffic going to or from the ZyWALL's VPN tunnels. It does not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). |
| External Database Service General Setup | The external database content filtering service has the ZyWALL check an external database to find to which category a requested web page belongs. |
| Enable External Database Content Filtering | Turn on external database content filtering to have the ZyWALL block or forward access to web pages depending on the ZyWALL's external database content filtering settings. |

**Table 56** SECURITY > CONTENT FILTER > General

| LABEL | DESCRIPTION |
|---|---|
| Matched Web Pages | Select **Block** to prevent users from accessing web pages that match the categories that you select below.<br>When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **CONTENT FILTER General** screen along with the category of the blocked web page.<br>Select **Log** to record attempts to access prohibited web pages. |
| Unrated Web Pages | Select **Block** to prevent users from accessing web pages that the external database content filtering has not categorized.<br>When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **CONTENT FILTER General** screen along with the category of the blocked web page.<br>Select **Log** to record attempts to access web pages that are not categorized. |
| When Content Filter Server Is Unavailable | Select **Block** to block access to any requested web page if the external content filtering database is unavailable. The following are possible causes:<br>There is no response from the external content filtering server within the time period specified in the **Content Filter Server Unavailable Timeout** field.<br>The ZyWALL is not able to resolve the domain name of the external content filtering database.<br>There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid").<br>Select **Log** to record attempts to access web pages that occur when the external content filtering database is unavailable. |
| Content Filter Server Unavailable Timeout | Specify a number of seconds (1 to 30) for the ZyWALL to wait for a response from the external content filtering server. If there is still no response by the time this period expires, the ZyWALL blocks or allows access to the requested web page based on the setting in the **Block When Content Filter Server Is Unavailable** field. |
| Enable Report Service | Select this option to record content filtering reports on myZyXEL.com. These reports consist of generated statistics and charts of access attempts to web sites belonging to the categories you selected in your content filter configuration. Click **Report** to go to myZyXEL.com. Then do the following to view the content filtering reports (see Chapter 13 on page 245 for details).<br>1. Log into myZyXEL.com and click your device's link to open it's **Service Management** screen.<br>2. Click **Content Filter** in the **Service Name** field to open the Blue Coat login screen.<br>3. Enter your ZyWALL's MAC address (in lower case) in the **Name** field. You can find this MAC address in the **Service Management** screen (Figure 161 on page 247). Type your myZyXEL.com account password in the **Password** field and click **Submit**. |
| External Database Service License Status | |

**Table 56** SECURITY > CONTENT FILTER > General

| LABEL | DESCRIPTION |
|---|---|
| License Status | This read-only field displays the status of your category-based content filtering (using an external database) service subscription.<br>**License Inactive** displays if you have not registered and activated the category-based content filtering service.<br>**License Active** and the subscription expiration date display if you have registered the ZyWALL and activated the category-based content filtering service.<br>**Trial Active** and the trial subscription expiration date display if you have registered the ZyWALL and activated the category-based content filtering service.<br>**License Inactive** and the date your subscription expired display if your subscription to the category-based content filtering service has expired.<br>Note: After you register for content filtering, you need to wait up to five minutes for content filtering to be activated. See Section 13.1 on page 245 for how to check the content filtering activation. |
| Message to display when a site is blocked | |
| Denied Access Message | Enter a message to be displayed when a user tries to access a restricted web site. The default message is Please contact your network administrator! |
| Redirect URL | Enter the URL of the web page to which you want to send users when their web access is blocked by content filtering. The web page you specify here opens in a new frame below the denied access message.<br>Use "http://" followed by up to 120 ASCII characters. For example, http://192.168.1.17/blocked access.<br>If you do not specify a URL and a user tries to access a web page containing a forbidden object, a blocking page displays on the forbidden object. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

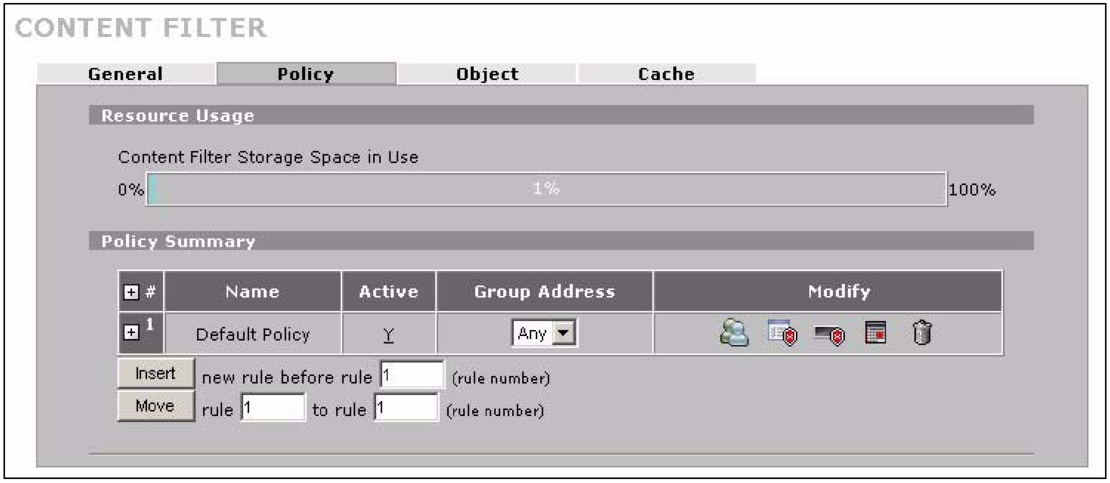
## 12.4 Content Filter Policy

Click **SECURITY** > **CONTENT FILTER** > **Policy** to display the following screen.

This screen lists groups of content filtering settings called policies. Content filtering policies allow you to have different content filtering settings for different users or groups of users. For example, you may want to block most employees from accessing finance or stock websites, but allow the finance department to access these. You can set the ZyWALL to use external database content filtering and select which web site categories to block and/or log.

You may find that a web site has not been accurately categorized or that a web site's contents have changed and the content filtering category needs to be updated. See Section 13.3 on page 250 for how to submit the web site for review.

**Figure 152** SECURITY > CONTENT FILTER > Policy



| # | Name | Active | Group Address | Modify |
|---|---|---|---|---|
| 1 | Default Policy | Y | Any | |

Insert new rule before rule 1 (rule number)

Move rule 1 to rule 1 (rule number)

The following table describes the labels in this screen.

**Table 57** SECURITY > CONTENT FILTER > Policy

| LABEL | DESCRIPTION |
|---|---|
| Content Filter Storage Space in Use | This bar displays the percentage of the ZyWALL's content filter policies storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary content filter policies before adding more. |
| The following fields summarize the content filter policies you have created. | |
| +/- | In the heading row, click + to expand or - to collapse the **Group Address** drop down lists for all of the displayed rules. |
| # | This is the content filter policy number. The ordering of your policies is important as rules are applied in turn. Click + to expand or - to collapse the **Group Address** drop down list. |
| Name | This is the name of the content filter policy. |
| Active | This field displays whether a content filter policy is turned on (**Y**) or not (**N**). Click the setting to change it. |
| Group Address | This drop-down list box displays the source (user) addresses or ranges of addresses to which the content filter policy applies. Please note that a blank source or destination address is equivalent to **Any**. |
| Modify | Click the general icon to restrict web features and edit the source (user) addresses or ranges of addresses to which the content filter policy applies.<br>Click the external database icon to edit which web features and content categories the content filter policy blocks.<br>Click the customization icon to configure the policy's list of good (allowed) web site addresses and a list of bad (blocked) web site addresses. You can also block web sites based on whether the web site's address contains a keyword.<br>Click the schedule icon to set for which days and times the policy applies.<br>Click the delete icon to remove the content filter policy. You cannot delete the default policy. A window display asking you to confirm that you want to delete the policy. Note that subsequent policies move up by one when you take this action. |

**Table 57** SECURITY > CONTENT FILTER > Policy (continued)

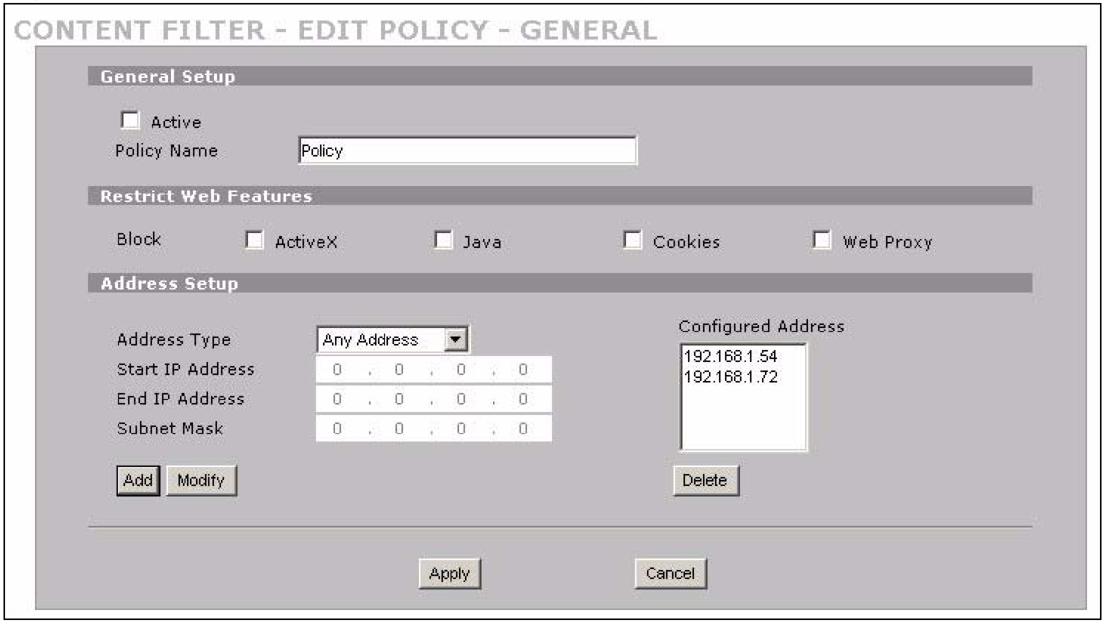
| LABEL | DESCRIPTION |
|---|---|
| Insert | Type the index number for where you want to put a content filter policy. For example, if you type 6, your new content filter policy becomes number 6 and the previous content filter policy 6 (if there is one) becomes content filter policy 7.<br>Click **Insert** to display the screens where you configure the content filter policy. |
| Move | Type a content filter policy's index number and the number for where you want to put that policy. Click **Move** to move the policy to the number that you typed. The ordering of your policies is important as they are applied in order of their numbering. |

## 12.5 Content Filter Policy: General

Click **SECURITY** > **CONTENT FILTER** > **Policy** and use the **Insert** button or a policy's general icon to display the following screen.

Use this screen to restrict web features and edit the source (user) addresses or ranges of addresses to which the content filter policy applies.

**Figure 153** SECURITY > CONTENT FILTER > Policy > General



CONTENT FILTER - EDIT POLICY - GENERAL

General Setup

☐ Active

Policy Name: Policy

Restrict Web Features

Block ☐ ActiveX ☐ Java ☐ Cookies ☐ Web Proxy

Address Setup

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Configured Address:
192.168.1.54
192.168.1.72

The following table describes the labels in this screen.

**Table 58** SECURITY > CONTENT FILTER > Policy > General

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this option to turn on the content filter policy. |
| Policy Name | Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the content filter policy. Spaces are allowed. |

**Table 58** SECURITY > CONTENT FILTER > Policy > General (continued)

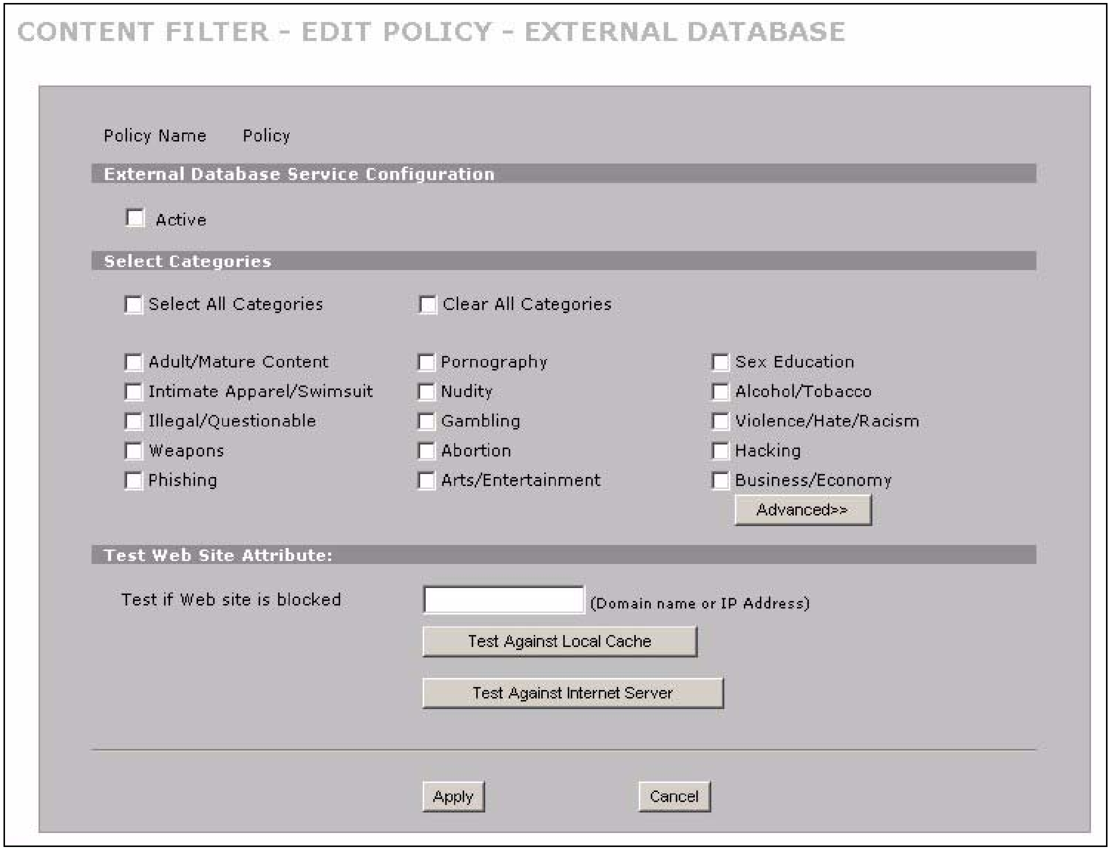
| LABEL | DESCRIPTION |
|---|---|
| Restrict Web Features | Select the check box(es) to restrict a feature. When you try to access a page containing a restricted feature, the whole page will be blocked or the restricted feature part of the web page will appear blank or grayed out. You will also see the message and URL you configured in the **Denied Access Message** and **Redirect URL** fields. |
| Block<br>ActiveX | ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again. |
| Java Applet | Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds. |
| Cookies | Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID. |
| Web Proxy | A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server. |
| Address Setup | |
| Address Type | Do you want the policy to apply to packets from a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**. |
| Start IP Address | Enter the single IP address or the starting IP address in a range here. |
| End IP Address | Enter the ending IP address in a range here. |
| Subnet Mask | Enter the subnet mask here, if applicable. |
| Add | Click **Add** to add a new address to the **Configured Address** box. You can add multiple addresses, ranges of addresses, and/or subnets. |
| Modify | To edit an existing source or destination address, select it from the box and click **Modify**. |
| Delete | Highlight an existing source or destination address from the **Configured Address** box and click **Delete** to remove it. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 12.6 Content Filter Policy: External Database

Click **SECURITY** > **CONTENT FILTER** > **Policy** and then a policy's external database icon to display the following screen.

Use this screen to edit which content categories the content filter policy blocks.

**Figure 154** SECURITY > CONTENT FILTER > Policy > External Database



CONTENT FILTER - EDIT POLICY - EXTERNAL DATABASE

Policy Name Policy

External Database Service Configuration

☐ Active

Select Categories

☐ Select All Categories ☐ Clear All Categories

☐ Adult/Mature Content
☐ Intimate Apparel/Swimsuit
☐ Illegal/Questionable
☐ Weapons
☐ Phishing
☐ Pornography
☐ Nudity
☐ Gambling
☐ Abortion
☐ Arts/Entertainment
☐ Sex Education
☐ Alcohol/Tobacco
☐ Violence/Hate/Racism
☐ Hacking
☐ Business/Economy

Test Web Site Attribute:

Test if Web site is blocked (Domain name or IP Address)

The following table describes the labels in this screen.

**Table 59** SECURITY > CONTENT FILTER > Policy > External Database

| LABEL | DESCRIPTION |
|---|---|
| Policy Name | This is the name of the content filter policy that you are configuring. |
| Active | Select this option to apply category based content filtering for this policy. |
| Select Categories | These are the categories available at the time of writing.<br>Note: If you chose to record attempts to access the restricted pages and a web page matches more than one category you selected, you will see a log showing this page matches one category (the first matched one) only. |
| Select All Categories | Select this check box to restrict access to all site categories listed below. |
| Clear All Categories | Select this check box to clear the selected categories below. |
| Adult/Mature Content | Selecting this category excludes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children. |
| Pornography | Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest. |

**Table 59** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Sex Education | Selecting this category excludes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement. |
| Intimate Apparel/Swimsuit | Selecting this category excludes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered. |
| Nudity | Selecting this category excludes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals. |
| Alcohol/Tobacco | Selecting this category excludes pages that promote or offer the sale alcohol/tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products. |
| Illegal/Questionable | Selecting this category excludes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers.<br>Note: This category includes sites identified as being malicious in any way (such as having viruses, spyware and etc.). |
| Gambling | Selecting this category excludes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements). |
| Violence/Hate/Racism | Selecting this category excludes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics. |
| Weapons | Selecting this category excludes pages that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. It does not include pages that promote collecting weapons, or groups that either support or oppose weapons use. |
| Abortion | Selecting this category excludes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion. |

**Table 59** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Hacking | Selecting this category excludes pages that distribute, promote, or provide hacking tools and/or information which may help gain unauthorized access to computer systems and/or computerized communication systems. Hacking encompasses instructions on illegal or questionable tactics, such as creating viruses, distributing cracked or pirated software, or distributing other protected intellectual property. |
| Phishing | Selecting this category excludes pages that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data (i.e. credit card numbers, pin numbers). |
| Arts/Entertainment | Selecting this category excludes pages that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment. |
| Business/Economy | Selecting this category excludes pages devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include pages that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services). |
| Alternative Spirituality/Occult | Selecting this category excludes pages that promote and provide information on religions such as Wicca, Witchcraft or Satanism. Occult practices, atheistic views, voodoo rituals or any other form of mysticism are represented here. Includes sites that endorse or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, incantations, curses and magic powers. This category includes sites which discuss or deal with paranormal or unexplained events. |
| Illegal Drugs | Selecting this category excludes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia. |
| Education | Selecting this category excludes pages that offer educational information, distance learning and trade school information or programs. It also includes pages that are sponsored by schools, educational facilities, faculty, or alumni groups. |
| Cultural/Charitable Organization | Selecting this category excludes pages that nurture cultural understanding and foster volunteerism such as 4H, the Lions and Rotary Clubs. Also encompasses non-profit associations that cultivate philanthropic or relief efforts. Sites that provide a learning environment or cultural refinement/awareness outside of the strictures of formalized education such as museums and planetariums are included under this heading. |
| Financial Services | Selecting this category excludes pages that provide or advertise banking services (online or offline) or other types of financial information, such as loans. It does not include pages that offer market information, brokerage or trading services. |
| Brokerage/Trading | Selecting this category excludes pages that provide or advertise trading of securities and management of investment assets (online or offline). It also includes insurance pages, as well as pages that offer financial investment strategies, quotes, and news. |
| Online Games | Selecting this category excludes pages that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. It also includes pages dedicated to selling board games as well as journals and magazines dedicated to game playing. It includes pages that support or host online sweepstakes and giveaways. |

**Table 59** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Government/Legal | Selecting this category excludes pages sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. It also includes pages that discuss or explain laws of various governmental entities. |
| Military | Selecting this category excludes pages that promote or provide information on military branches or armed services. |
| Political/Activist Groups | Selecting this category excludes pages sponsored by or which provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities. |
| Health | Selecting this category excludes pages that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complimentary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition. |
| Computers/Internet | Selecting this category excludes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies. |
| Search Engines/Portals | Selecting this category excludes pages that support searching the Internet, indices, and directories. |
| Spyware/Malware Sources | Selecting this category excludes pages which distribute spyware and other malware. Spyware is defined as software which takes control of your computer, modifies computer settings, collects or reports personal information, or misrepresents itself by tricking users to install, download, or enter personal information. This includes drive-by downloads; browser hijackers; dialers; intrusive advertising; any program which modifies your homepage, bookmarks, or security settings; and keyloggers. It also includes any software which bundles spyware (as defined above) as part of its offering. Information collected or reported is "personal" if it contains uniquely identifying data, such as email addresses, name, social security number, IP address, etc. A site is not classified as spyware if the user is reasonably notified that the software will perform these actions (ie, it alerts that it will send personal information, be installed, or that it will log keystrokes). Note: Sites rated as spyware should have a second category assigned with them. |
| Spyware Effects/Privacy Concerns | Selecting this category excludes pages to which spyware (as defined in the Spyware/Malware Sources category) reports its findings or from which it alone downloads advertisements. Also includes sites that contain serious privacy issues, such as “phone home” sites to which software can connect and send user info; sites that make extensive use of tracking cookies without a posted privacy statement; and sites to which browser hijackers redirect users. Usually does not include sites that can be marked as Spyware/Malware. Note: Sites rated as spyware effects typically have a second category assigned with them. |
| Job Search/Careers | Selecting this category excludes pages that provide assistance in finding employment, and tools for locating prospective employers. |
| News/Media | Selecting this category excludes pages that primarily report information or comments on current events or contemporary issues of the day. It also includes radio stations and magazines. It does not include pages that can be rated in other categories. |
| Personals/Dating | Selecting this category excludes pages that promote interpersonal relationships. |

**Table 59** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Reference | Selecting this category excludes pages containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related pages and scientific information. |
| Open Image/Media Search | Selecting this category excludes pages with image or video search capabilities which return graphical results (i.e. thumbnail pictures) that include potentially pornographic content along with non-pornographic content (as defined in the Pornography category). Sites that explicitly exclude offensive content are not included in this category. |
| Chat/Instant Messaging | Selecting this category excludes pages that provide chat or instant messaging capabilities or client downloads. |
| Email | Selecting this category excludes pages offering web-based email services, such as online email reading, e-cards, and mailing list services. |
| Blogs/Newsgroups | Selecting this category excludes pages that offer access to Usenet news groups or other messaging or bulletin board systems. Also, blog specific sites or an individual with his own blog. This does not include social networking communities with blogs. |
| Religion | Selecting this category excludes pages that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. It does not include pages containing alternative religions such as Wicca or witchcraft (Cult/Occult) or atheist beliefs (Political/Activist Groups). |
| Social Networking | Selecting this category excludes pages that enable people to connect with others to form an online community. Typically members describe themselves in personal web page policies and form interactive networks, linking them with other members based on common interests or acquaintances. Instant messaging, file sharing and web logs (blogs) are common features of Social Networking sites. Note: These sites may contain offensive material in the community-created content. Sites in this category are also referred to as "virtual communities" or "online communities". This category does not include more narrowly focused sites, like those that specifically match descriptions for Personals/ Dating sites or Business sites. |
| Online Storage | Selecting this category excludes pages that provide a secure, encrypted, off-site backup and restoration of personal data. These online repositories are typically used to store, organize and share videos, music, movies, photos, documents and other electronically formatted information. Sites that fit this criteria essentially act as your personal hard drive on the Internet. |
| Remote Access Tools | Selecting this category excludes pages that primarily focus on providing information about and/or methods that enables authorized access to and use of a desktop computer or private network remotely. |
| Shopping | Selecting this category excludes pages that provide or advertise the means to obtain goods or services. It does not include pages that can be classified in other categories (such as vehicles or weapons). |
| Auctions | Selecting this category excludes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements. |
| Real Estate | Selecting this category excludes pages that provide information on renting, buying, or selling real estate or properties. |

**Table 59** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Society/Lifestyle | Selecting this category excludes pages providing information on matters of daily life. This does not include pages relating to entertainment, sports, jobs, sex or pages promoting alternative lifestyles such as homosexuality. Personal homepages fall within this category if they cannot be classified in another category. |
| Sexuality/Alternative Lifestyles | Selecting this category excludes pages that provide information, promote, or cater to gays, lesbians, swingers, other sexual orientations or practices, or a particular fetish. This category does not include sites that are sexually gratuitous in nature which would typically fall under the Pornography category. |
| Restaurants/Dining/Food | Selecting this category excludes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes. |
| Sports/Recreation/Hobbies | Selecting this category excludes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting. |
| Travel | Selecting this category excludes pages that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos. |
| Vehicles | Selecting this category excludes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts. |
| Humor/Jokes | Selecting this category excludes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/Mature content also have an Adult/Mature category rating. |
| Software Downloads | Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge. |
| Pay to Surf | Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages. |
| Peer-to-Peer | Selecting this category excludes pages that distribute software to facilitate the direct exchange of files between users, including software that enables file search and sharing across a network without dependence on a central server. |
| Streaming Media/MP3s | Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including sites that provide downloads for such viewers. |
| Proxy Avoidance | Selecting this category excludes pages that provide information on how to bypass proxy server/appliance features or gain access to URLs in any way that bypasses the proxy server/appliance. It also includes any service that will allow a person to bypass the content filtering feature, such as anonymous surfing services. |
| For Kids | Selecting this category excludes pages designed specifically for children. |
| Web Advertisements | Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements. |

**Table 59** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Web Hosting | Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services. |
| Advanced/Basic | Click **Advanced** to see an expanded list of categories, or click **Basic** to see a smaller list. |
| Test Web Site Attribute | |
| Test if Web site is blocked | You can check whether or not the content filter policy currently blocks any given web page. Enter a web site URL in the text box. |
| Test Against Local Cache | Click this button to test whether or not the web site above is saved in the ZyWALL's database of restricted web pages. |
| Test Against Internet Server | Click this button to test whether or not the web site above is saved in the external content filter server's database of restricted web pages. |
| Apply | Click **Apply** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

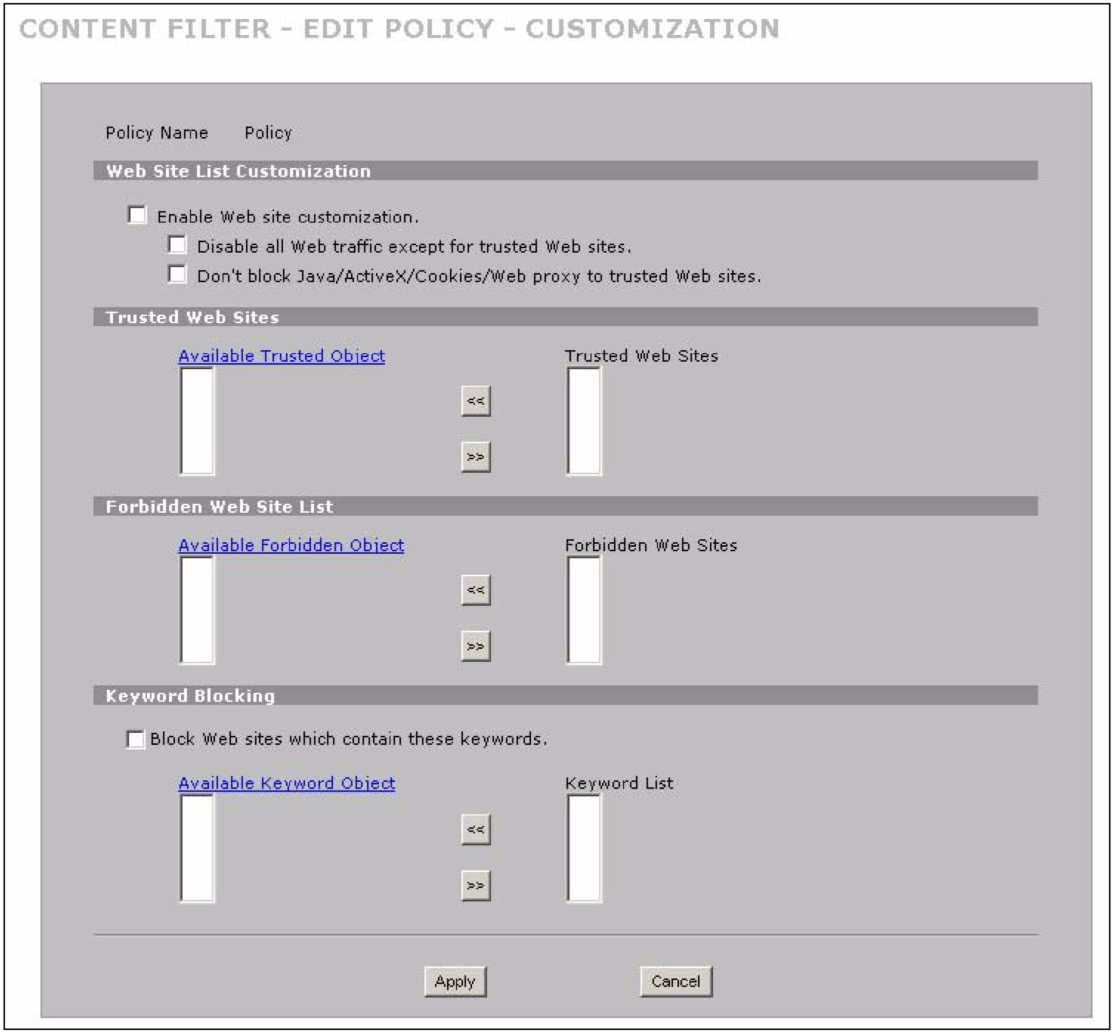
## 12.7 Content Filter Policy: Customization

Click **SECURITY** > **CONTENT FILTER** > **Policy** and then a policy's customization icon to display the following screen.

Use this screen to select good (allowed) web site addresses for this policy and bad (blocked) web site addresses. You can also block web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

Use the **SECURITY** > **CONTENT FILTER** > **Object** screen (see Section 12.9 on page 240) first to configure the master lists of trusted (allowed) web sites, forbidden (blocked) web sites, and keywords.

**Figure 155** SECURITY > CONTENT FILTER > Policy > Customization


CONTENT FILTER - EDIT POLICY - CUSTOMIZATION
Policy Name
Policy
Web Site List Customization
☐ Enable Web site customization.
☐ Disable all Web traffic except for trusted Web sites.
☐ Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites.
Trusted Web Sites
Available Trusted Object
Trusted Web Sites
<<
>>
Forbidden Web Site List
Available Forbidden Object
Forbidden Web Sites
<<
>>
Keyword Blocking
☐ Block Web sites which contain these keywords.
Available Keyword Object
Keyword List
<<
>>
Apply
Cancel

The following table describes the labels in this screen.

**Table 60** SECURITY > CONTENT FILTER > Policy > Customization

| LABEL | DESCRIPTION |
|---|---|
| Policy Name | This is the name of the content filter policy that you are configuring. |
| Web Site List Customization | |
| Enable Web site customization | Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names. |
| Disable all Web traffic except for trusted Web sites | When this box is selected, the ZyWALL only allows Web access to sites on the **Trusted Web Site** list. If they are chosen carefully, this is the most effective way to block objectionable material. |
| Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites | When this box is selected, the ZyWALL will permit Java, ActiveX and Cookies from sites on the **Trusted Web Site** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted. |

**Table 60** SECURITY > CONTENT FILTER > Policy > Customization (continued)

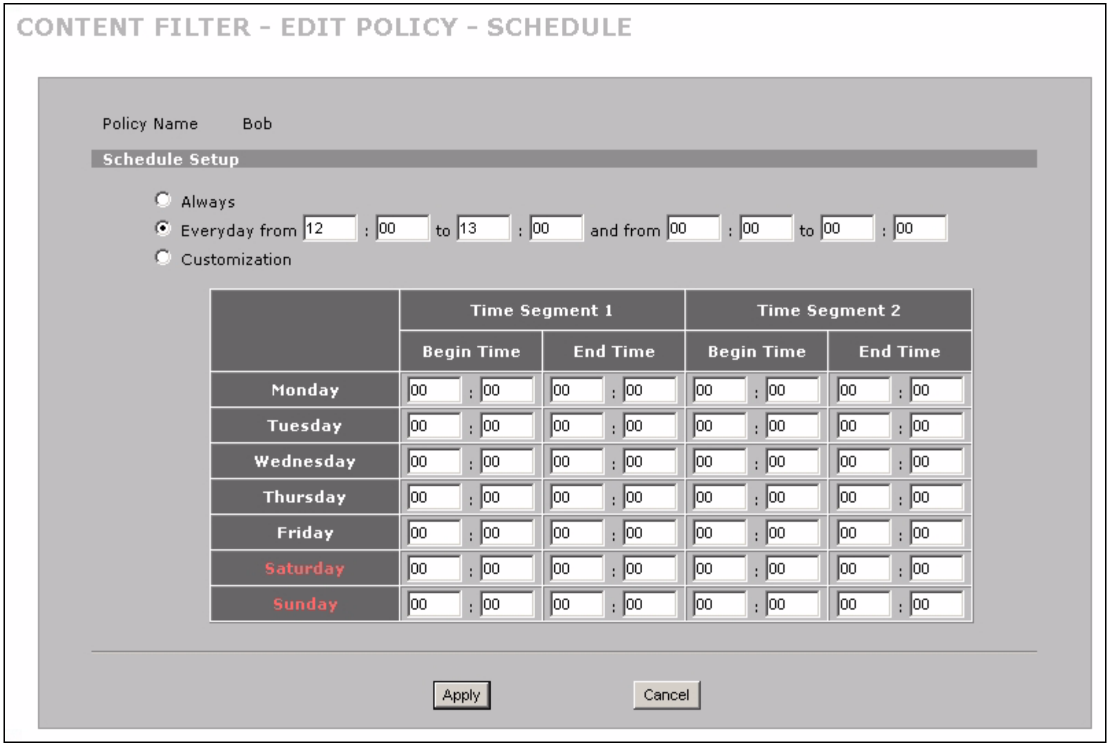
| LABEL | DESCRIPTION |
|---|---|
| Available Trusted Object | This list displays the trusted host names you configured in the **SECURITY > CONTENT FILTER > Object** screen (click **Available Trusted Object** to go there). Select the ones to which you want to allow access and use the arrow button to move them to the **Trusted Web Sites** list. |
| Trusted Web Sites | This list displays web sites to which this content filtering policy allows access. Select an entry and use the arrow button to remove it from the list. |
| Available Forbidden Object | This list displays the forbidden host names you configured in the **SECURITY > CONTENT FILTER > Object** screen (click **Available Forbidden Object** to go there). Select the ones you want this policy to block and use the arrow button to move them to the **Forbidden Web Sites** list. |
| Forbidden Web Sites | This list displays web sites to which this content filtering policy blocks access. Select an entry and use the arrow button to remove it from the list. |
| Keyword Blocking | Keyword blocking allows you to block websites with URLs that contain certain keywords in the domain name or IP address.<br>See Section 12.10 on page 242 for how to set how much of the URL the ZyWALL checks. |
| Block Web sites which contain these keywords. | Select this checkbox to enable keyword blocking. |
| Available Keyword Object | This list displays the keywords you configured in the **SECURITY > CONTENT FILTER > Object** screen (click **Available Keyword Object** to go there). Select the ones you want this policy to block and use the arrow button to move them to **Keyword List**. |
| Keyword List | This list displays the keywords that this content filtering policy blocks. Select an entry and use the arrow button to remove it from the list. |
| Apply | Click **Apply** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 12.8 Content Filter Policy: Schedule

Click **SECURITY** > **CONTENT FILTER** > **Policy** and then a policy's schedule icon to display the following screen.

Use this screen to set for which days and times the policy applies.

**Figure 156** SECURITY > CONTENT FILTER > Policy > Schedule



CONTENT FILTER - EDIT POLICY - SCHEDULE

Policy Name Bob

Schedule Setup

○ Always
● Everyday from 12 : 00 to 13 : 00 and from 00 : 00 to 00 : 00
○ Customization

| | Time Segment 1 | | Time Segment 2 | |
|---|---|---|---|---|
| | Begin Time | End Time | Begin Time | End Time |
| Monday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Tuesday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Wednesday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Thursday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Friday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Saturday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |
| Sunday | 00 : 00 | 00 : 00 | 00 : 00 | 00 : 00 |

The following table describes the labels in this screen.

**Table 61** SECURITY > CONTENT FILTER > Policy > Schedule

| LABEL | DESCRIPTION |
|---|---|
| Policy Name | This is the name of the content filter policy that you are configuring. |
| Schedule Setup | Content filtering scheduling applies to the filter list, customized sites and keywords. Restricted web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. |
| Always | Select this option to have content filtering active all the time. |
| Everyday from/to | Select this option to have content filtering active during the specified time interval(s) of each day. In the **from** and **to** fields, enter the time period(s), in 24-hour format, during which content filtering will be enforced. |
| Customization | Select this option to have content filtering only active during the specified time interval(s) of the specified day(s). In the **Begin Time** and **End Time** fields, enter the time period(s), in 24-hour format, for individual day(s) of the week. |
| Apply | Click **Apply** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

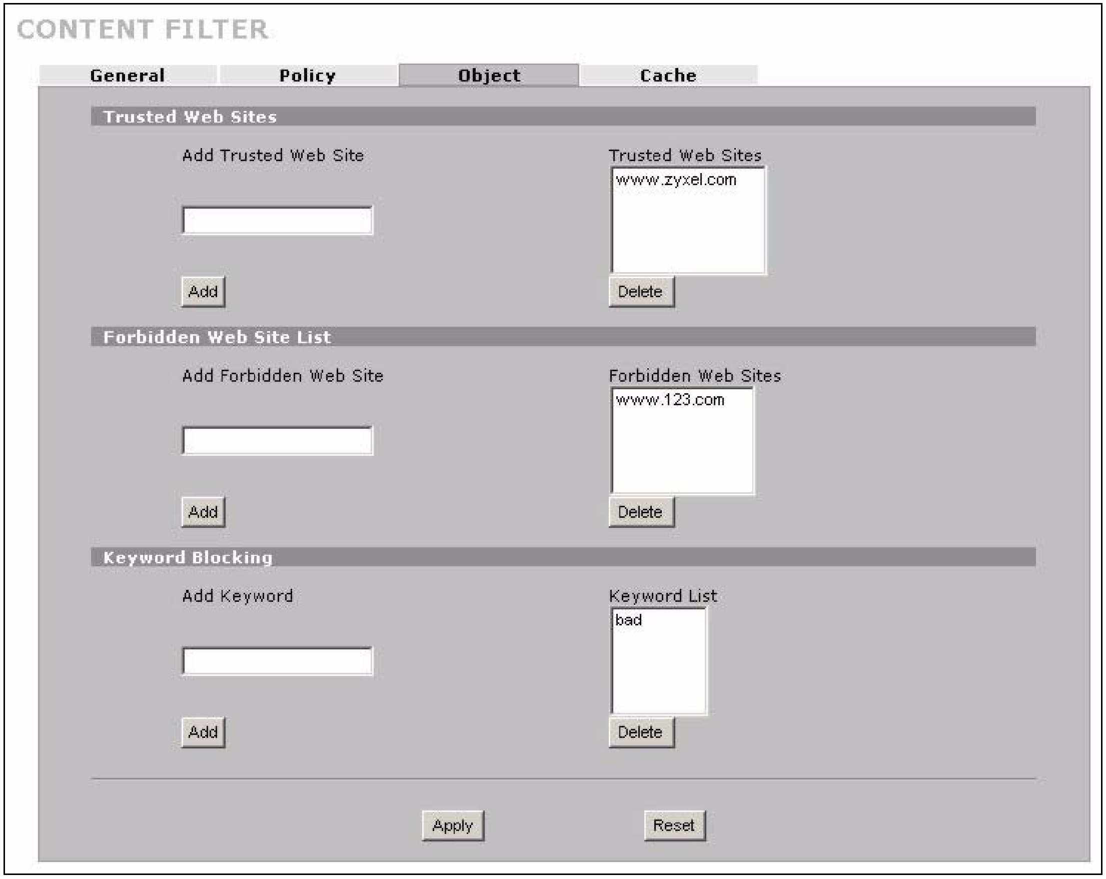
## 12.9 Content Filter Object

Click **SECURITY** > **CONTENT FILTER** > **Object** to display the following screen.

Use this screen to a list of allowed web site addresses for this policy and a list of blocked web site addresses. You can also block web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

To use this screens settings in content filtering, you must use the **SECURITY > CONTENT FILTER > Policy > Customization** screen to set individual policies to add or remove specific sites or keywords for individual policies.

**Figure 157** SECURITY > CONTENT FILTER > Object


CONTENT FILTER
General
Policy
Object
Cache
Trusted Web Sites
Add Trusted Web Site
Trusted Web Sites
www.zyxel.com
Add
Delete
Forbidden Web Site List
Add Forbidden Web Site
Forbidden Web Sites
www.123.com
Add
Delete
Keyword Blocking
Add Keyword
Keyword List
bad
Add
Delete
Apply
Reset

The following table describes the labels in this screen.

**Table 62** SECURITY > CONTENT FILTER > Object

| LABEL | DESCRIPTION |
|---|---|
| Trusted Web Sites | These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries. |
| Add Trusted Web Site | Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are allowed. For example, entering “zyxel.com” also allows “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, etc. |
| Trusted Web Sites | This list displays the trusted web sites already added. |
| Add | Click this button when you have finished adding the host name in the text field above. |
| Delete | Select a web site name from the **Trusted Web Site** list, and then click this button to delete it from that list. |

**Table 62** SECURITY > CONTENT FILTER > Object (continued)

| LABEL | DESCRIPTION |
|---|---|
| Forbidden Web Site List | Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries. |
| Add Forbidden Web Site | Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are blocked. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", etc. |
| Forbidden Web Sites | This list displays the forbidden web sites already added. |
| Add | Click this button when you have finished adding the host name in the text field above. |
| Delete | Select a web site name from the **Forbidden Web Site** list, and then click this button to delete it from that list. |
| Keyword Blocking | **Keyword Blocking** allows you to block websites with URLs that contain certain keywords in the domain name or IP address.<br>See Section 12.10 on page 242 for how to set how much of the URL the ZyWALL checks. |
| Add Keyword | Enter a keyword (up to 31 printable ASCII characters) to block. You can also enter a numerical IP address. |
| Keyword List | This list displays the keywords already added. |
| Add | Click this button when you have finished adding the key words field above. |
| Delete | Select a keyword from the **Keyword List**, and then click this button to delete it from that list. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.10 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

### 12.10.1 Domain Name or IP Address URL Checking

By default, the ZyWALL checks the URL's domain name or IP address when performing keyword blocking.

This means that the ZyWALL checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

### 12.10.2 Full Path URL Checking

Full path URL checking has the ZyWALL check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

### 12.10.3 File Name URL Checking

Filename URL checking has the ZyWALL check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

## 12.11 Content Filtering Cache

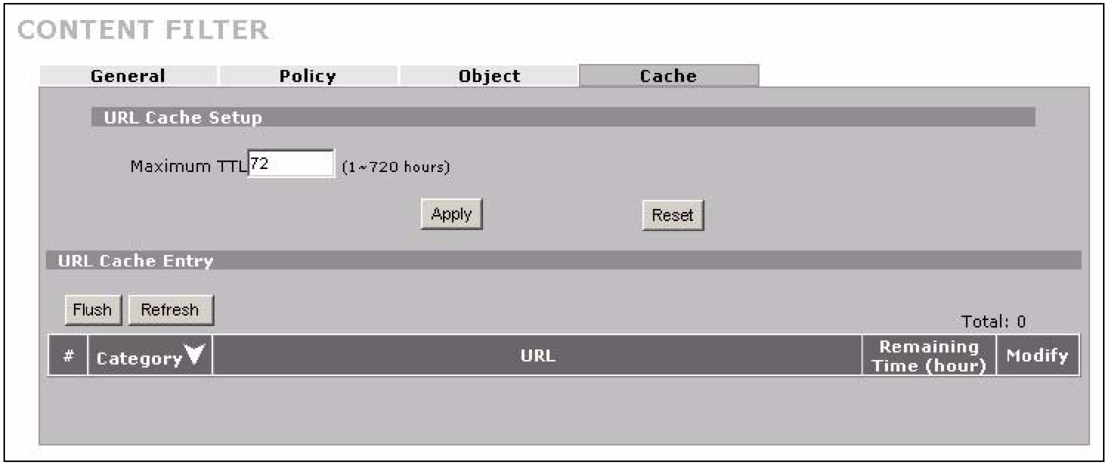
Click **SECURITY > CONTENT FILTER > Cache** to display the **CONTENT FILTER Cache** screen.

Use this screen to view and configure your ZyWALL’s URL caching. You can also configure how long a categorized web site address remains in the cache as well as view those web site addresses to which access has been allowed or blocked based on the responses from the external content filtering server. The ZyWALL only queries the external content filtering database for sites not found in the cache.

You can remove individual entries from the cache. When you do this, the ZyWALL queries the external content filtering database the next time someone tries to access that web site. This allows you to check whether a web site’s category has been changed.

Please see Section 13.3 on page 250 for how to submit a web site that has been incorrectly categorized.

**Figure 158** SECURITY > CONTENT FILTER > Cache


CONTENT FILTER
General
Policy
Object
Cache
URL Cache Setup
Maximum TTL 72 (1~720 hours)
Apply
Reset
URL Cache Entry
Flush
Refresh
Total: 0
#
Category
URL
Remaining Time (hour)
Modify

The following table describes the labels in this screen.

**Table 63** SECURITY > CONTENT FILTER > Cache

| LABEL | DESCRIPTION |
|---|---|
| URL Cache Setup | |
| Maximum TTL | Type the maximum time to live (TTL) (1 to 720 hours). This sets how long the ZyWALL is to allow an entry to remain in the URL cache before discarding it. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| URL Cache Entry | |
| Flush | Click this button to clear all web site addresses from the cache manually. |
| Refresh | Click this button to reload the cache. |
| # | This is the index number of a categorized web site address record. |
| Category | This field shows the site category to which requested access belongs. |
| URL | This is a web site's address that the ZyWALL previously checked with the external content filtering database. |
| Remaining Time (hour) | This is the number of hours left before the URL entry is discarded from the cache. |
| Modify | Click the delete icon to remove the URL entry from the cache. |

# 13

# Content Filtering Reports

This chapter describes how to view content filtering reports after you have activated the category-based content filtering subscription service.

See Chapter 5 on page 127 on how to create a myZyXEL.com account, register your device and activate the subscription services using the **REGISTRATION** screens.

## 13.1 Checking Content Filtering Activation

After you activate content filtering, you need to wait up to five minutes for content filtering to be turned on.

Since there will be no content filtering activation notice, you can do the following to see if content filtering is active.

1. Go to your device's web configurator's **CONTENT FILTER Categories** screen.
2. Select at least one category and click **Apply**.
3. Enter a valid URL or IP address of a web site in the **Test if Web site is blocked** field and click the **Test Against Internet Server** button.
   When content filtering is active, you should see an access blocked or access forwarded message. An error message displays if content filtering is not active.

## 13.2 Viewing Content Filtering Reports

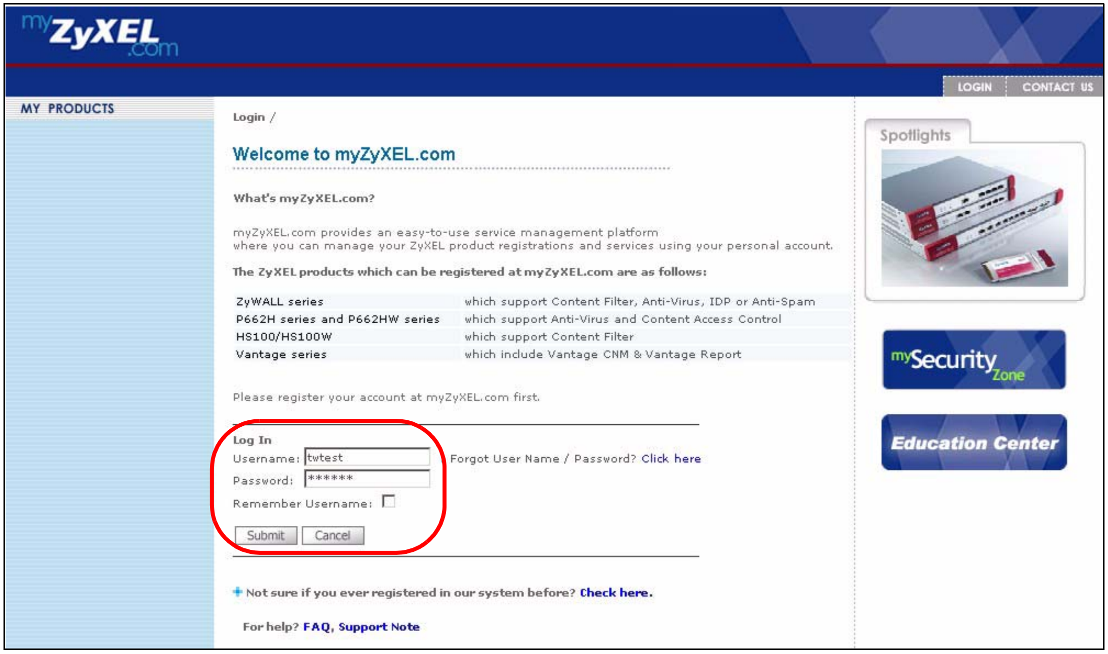
Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen.

You need to register your iCard before you can view content filtering reports.

Alternatively, you can also view content filtering reports during the free trial (up to 30 days).

1. Go to http://www.myZyXEL.com.
2. Fill in your myZyXEL.com account information and click **Submit**.

**Figure 159** myZyXEL.com: Login



Login /

Welcome to myZyXEL.com

What's myZyXEL.com?

myZyXEL.com provides an easy-to-use service management platform where you can manage your ZyXEL product registrations and services using your personal account.

The ZyXEL products which can be registered at myZyXEL.com are as follows:

| | |
|---|---|
| ZyWALL series | which support Content Filter, Anti-Virus, IDP or Anti-Spam |
| P662H series and P662HW series | which support Anti-Virus and Content Access Control |
| HS100/HS100W | which support Content Filter |
| Vantage series | which include Vantage CNM & Vantage Report |

Please register your account at myZyXEL.com first.

Log In
Username: twtest
Password: ******
Remember Username: ☐
Submit Cancel

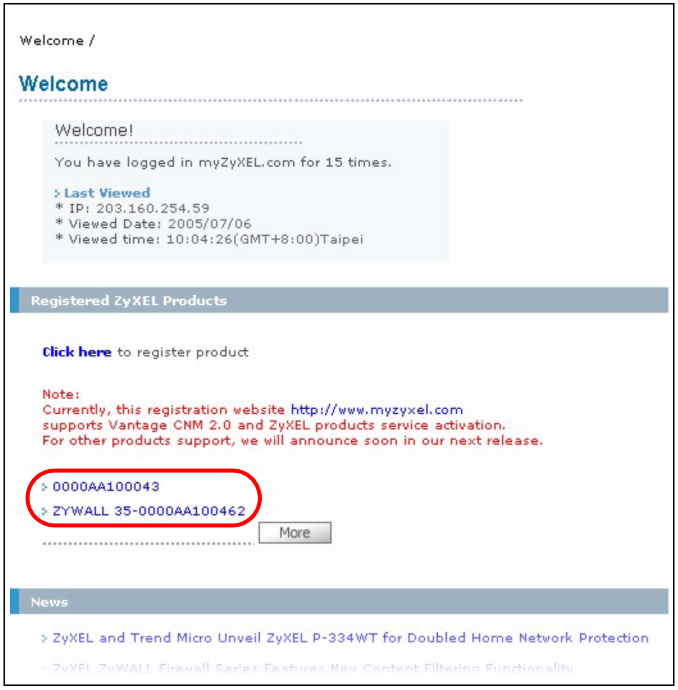
Forgot User Name / Password? Click here

Not sure if you ever registered in our system before? Check here.

For help? FAQ, Support Note

3 A welcome screen displays. Click your ZyWALL's model name and/or MAC address under **Registered ZyXEL Products**. You can change the descriptive name for your ZyWALL using the **Rename** button in the **Service Management** screen (see Figure 161 on page 247).

**Figure 160** myZyXEL.com: Welcome



Welcome /

Welcome

Welcome!

You have logged in myZyXEL.com for 15 times.

Last Viewed
* IP: 203.160.254.59
* Viewed Date: 2005/07/06
* Viewed time: 10:04:26(GMT+8:00)Taipei

Registered ZyXEL Products

Click here to register product

Note:
Currently, this registration website http://www.myzyxel.com supports Vantage CNM 2.0 and ZyXEL products service activation.
For other products support, we will announce soon in our next release.

- 0000AA100043
- ZYWALL 35-0000AA100462

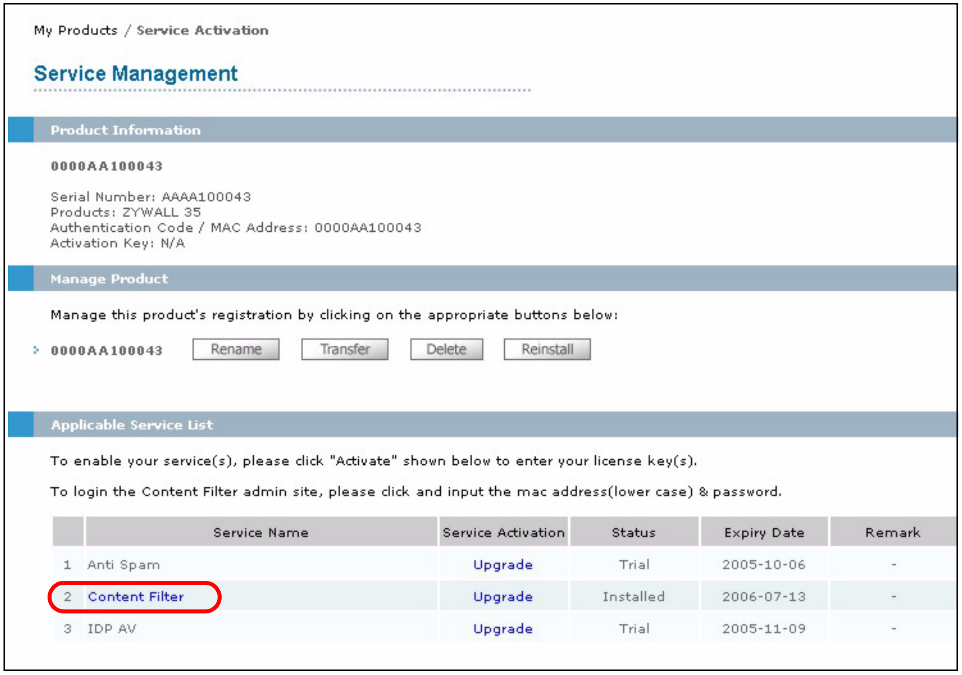
More

News

- ZyXEL and Trend Micro Unveil ZyXEL P-334WT for Doubled Home Network Protection
- ZyXEL ZyWALL Firewall Series Features New Content Filtering Functionality

4 In the **Service Management** screen click **Content Filter** in the **Service Name** field to open the Blue Coat login screen.

**Figure 161** myZyXEL.com: Service Management



My Products / Service Activation

Service Management

Product Information

0000AA100043

Serial Number: AAAA100043
Products: ZYWALL 35
Authentication Code / MAC Address: 0000AA100043
Activation Key: N/A

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

0000AA100043

Applicable Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

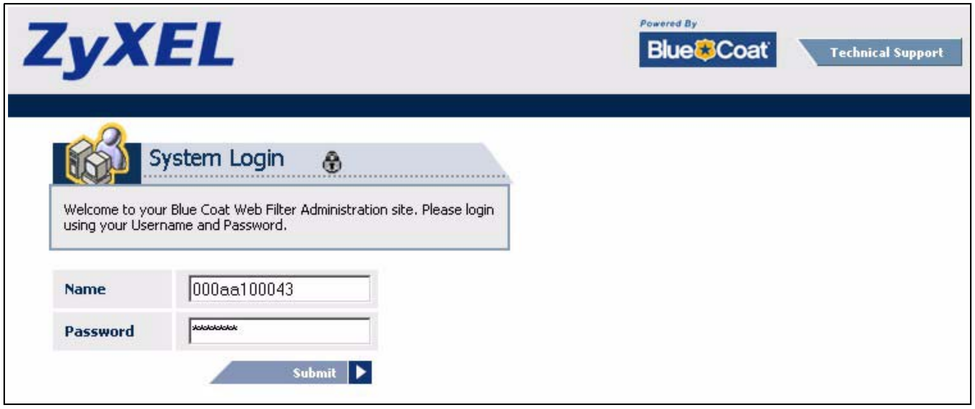
To login the Content Filter admin site, please click and input the mac address(lower case) & password.

| | Service Name | Service Activation | Status | Expiry Date | Remark |
|---|---|---|---|---|---|
| 1 | Anti Spam | Upgrade | Trial | 2005-10-06 | - |
| 2 | Content Filter | Upgrade | Installed | 2006-07-13 | - |
| 3 | IDP AV | Upgrade | Trial | 2005-11-09 | - |

5 Enter your ZyXEL device's MAC address (in lower case) in the **Name** field. You can find this MAC address in the **Service Management** screen (Figure 161 on page 247). Type your myZyXEL.com account password in the **Password** field.

6 Click **Submit**.

**Figure 162** Blue Coat: Login



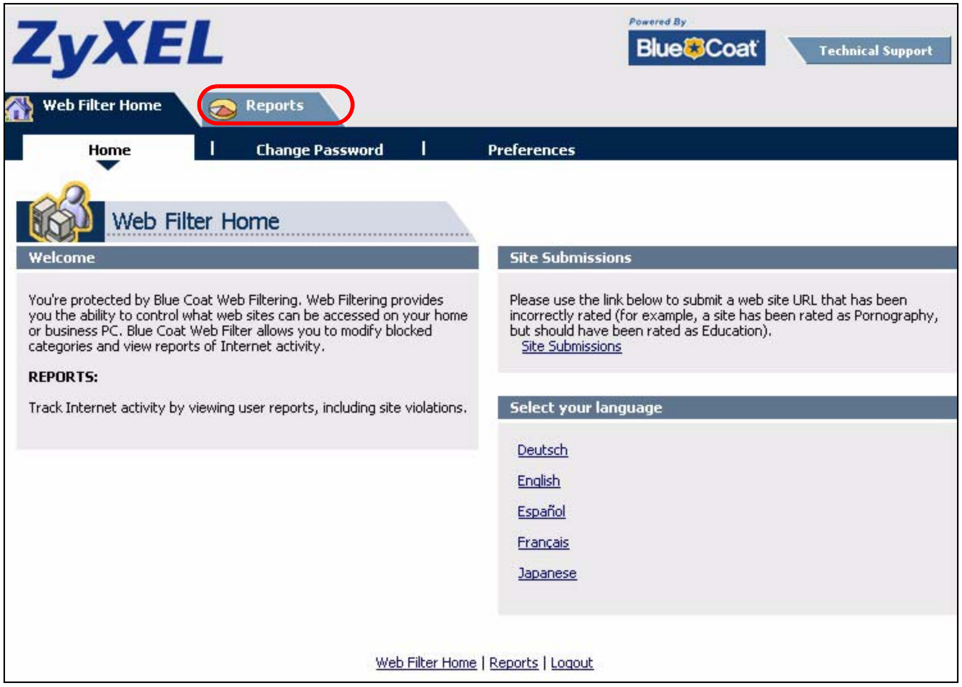
Welcome to your Blue Coat Web Filter Administration site. Please login using your Username and Password.

Name: 000aa100043

Password: *******

7 In the **Web Filter Home** screen, click the **Reports** tab.

**Figure 163** Content Filtering Reports Main Screen


ZyXEL
Powered By
BlueCoat
Technical Support
Web Filter Home
Reports
Home
Change Password
Preferences
Web Filter Home

**Welcome**

You're protected by Blue Coat Web Filtering. Web Filtering provides you the ability to control what web sites can be accessed on your home or business PC. Blue Coat Web Filter allows you to modify blocked categories and view reports of Internet activity.

**REPORTS:**

Track Internet activity by viewing user reports, including site violations.

**Site Submissions**

Please use the link below to submit a web site URL that has been incorrectly rated (for example, a site has been rated as Pornography, but should have been rated as Education).
Site Submissions

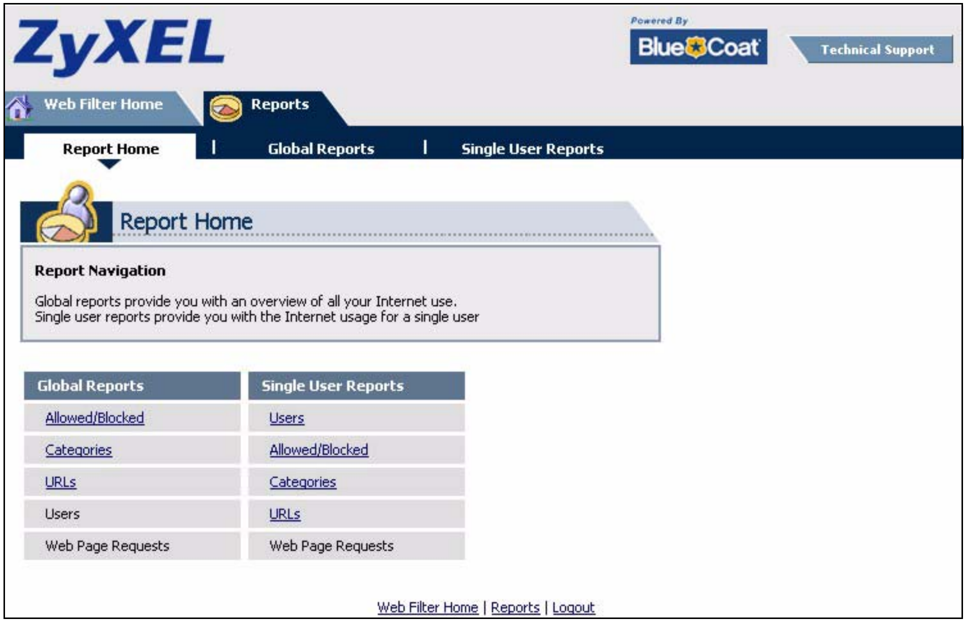
**Select your language**

Deutsch
English
Español
Français
Japanese

Web Filter Home | Reports | Logout

8 Select items under **Global Reports** or **Single User Reports** to view the corresponding reports.

**Figure 164** Blue Coat: Report Home


ZyXEL
Powered By
BlueCoat
Technical Support
Web Filter Home
Reports
Report Home
Global Reports
Single User Reports
Report Home

**Report Navigation**

Global reports provide you with an overview of all your Internet use.
Single user reports provide you with the Internet usage for a single user

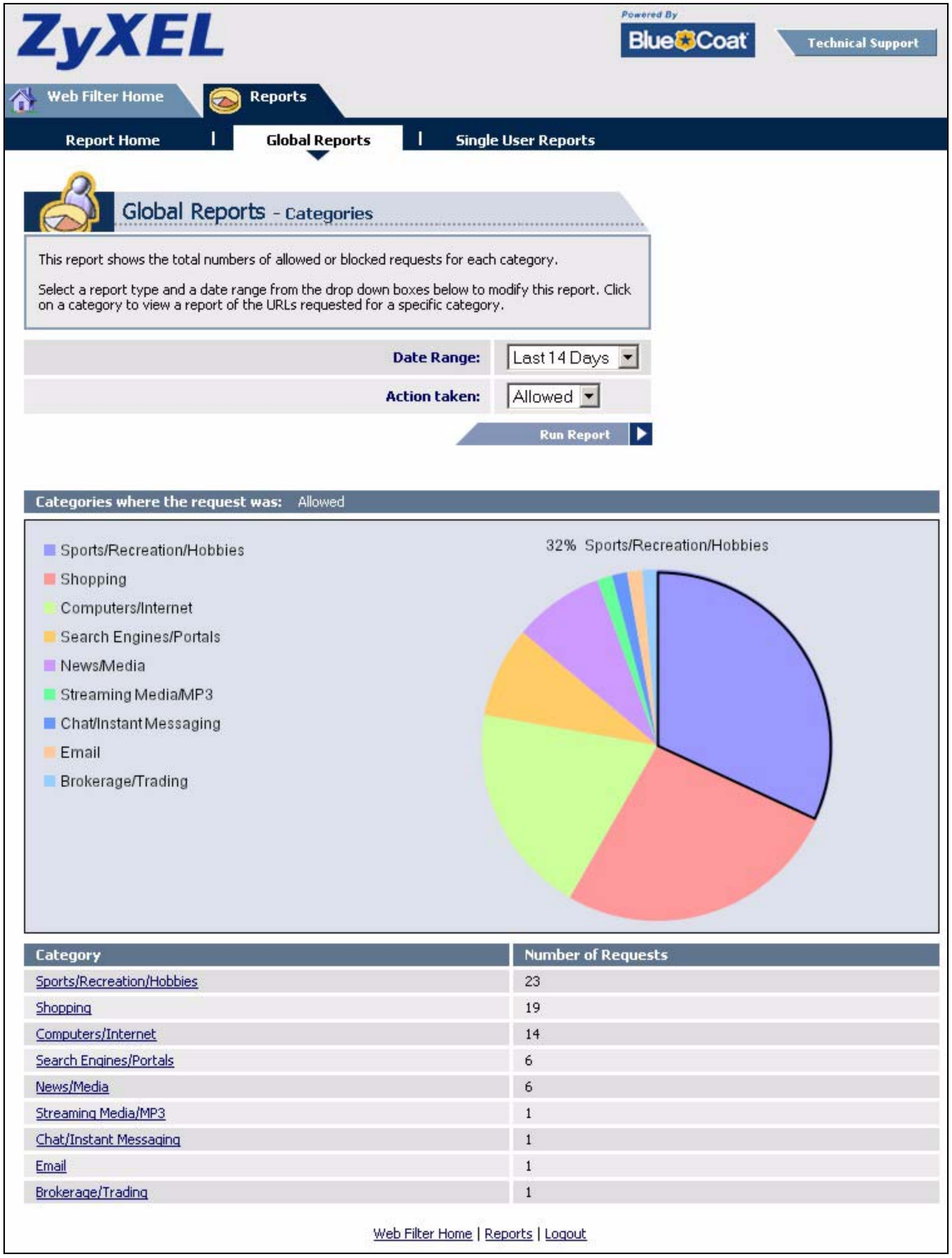
| Global Reports | Single User Reports |
|---|---|
| Allowed/Blocked | Users |
| Categories | Allowed/Blocked |
| URLs | Categories |
| Users | URLs |
| Web Page Requests | Web Page Requests |

Web Filter Home | Reports | Logout

9 Select a time period in the **Date Range** field, either **Allowed** or **Blocked** in the **Action Taken** field and a category (or enter the user name if you want to view single user reports) and click **Run Report**.The screens vary according to the report type you selected in the **Report Home** screen.

10 A chart and/or list of requested web site categories display in the lower half of the screen.

**Figure 165** Global Report Screen Example


Powered By
Technical Support
Web Filter Home
Reports
Report Home
Global Reports
Single User Reports
Run Report
Sports/Recreation/Hobbies
Shopping
Computers/Internet
Search Engines/Portals
News/Media
Streaming Media/MP3
Chat/Instant Messaging
Email
Brokerage/Trading
32% Sports/Recreation/Hobbies
Web Filter Home | Reports | Logout

Global Reports - Categories

This report shows the total numbers of allowed or blocked requests for each category.

Select a report type and a date range from the drop down boxes below to modify this report. Click on a category to view a report of the URLs requested for a specific category.

**Date Range:** Last 14 Days

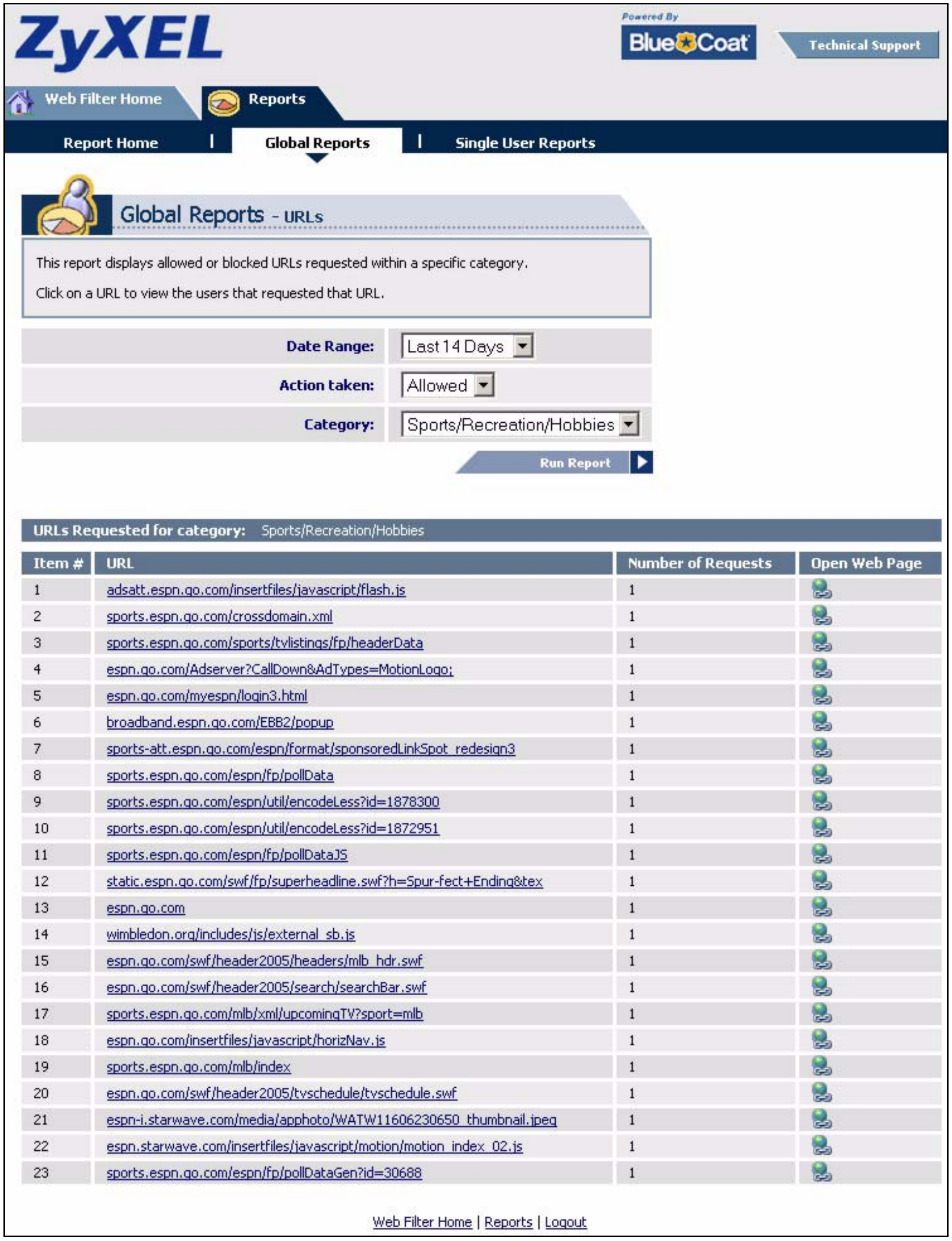
**Action taken:** Allowed

**Categories where the request was:** Allowed

| Category | Number of Requests |
|---|---|
| Sports/Recreation/Hobbies | 23 |
| Shopping | 19 |
| Computers/Internet | 14 |
| Search Engines/Portals | 6 |
| News/Media | 6 |
| Streaming Media/MP3 | 1 |
| Chat/Instant Messaging | 1 |
| Email | 1 |
| Brokerage/Trading | 1 |

**11** You can click a category in the **Categories** report or click **URLs** in the **Report Home** screen to see the URLs that were requested.

**Figure 166** Requested URLs Example



This report displays allowed or blocked URLs requested within a specific category.

Click on a URL to view the users that requested that URL.

Date Range: Last 14 Days

Action taken: Allowed

Category: Sports/Recreation/Hobbies

URLs Requested for category: Sports/Recreation/Hobbies

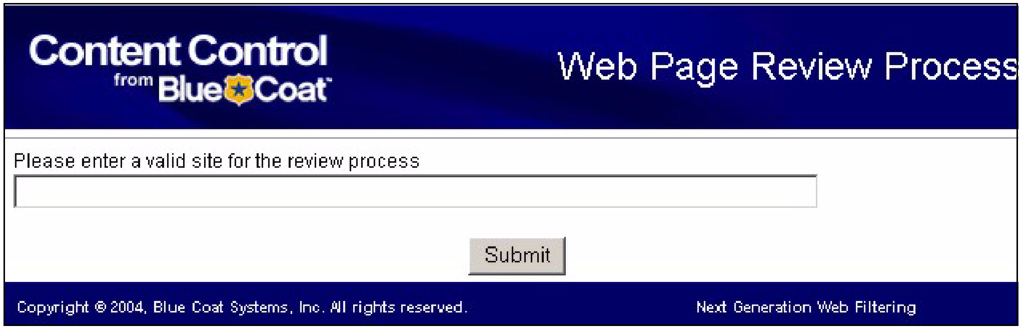
| Item # | URL | Number of Requests | Open Web Page |
|---|---|---|---|
| 1 | adsatt.espn.go.com/insertfiles/javascript/flash.js | 1 | 🔗 |
| 2 | sports.espn.go.com/crossdomain.xml | 1 | 🔗 |
| 3 | sports.espn.go.com/sports/tvlistings/fp/headerData | 1 | 🔗 |
| 4 | espn.go.com/Adserver?CallDown&AdTypes=MotionLogo; | 1 | 🔗 |
| 5 | espn.go.com/myespn/login3.html | 1 | 🔗 |
| 6 | broadband.espn.go.com/EBB2/popup | 1 | 🔗 |
| 7 | sports-att.espn.go.com/espn/format/sponsoredLinkSpot_redesign3 | 1 | 🔗 |
| 8 | sports.espn.go.com/espn/fp/pollData | 1 | 🔗 |
| 9 | sports.espn.go.com/espn/util/encodeLess?id=1878300 | 1 | 🔗 |
| 10 | sports.espn.go.com/espn/util/encodeLess?id=1872951 | 1 | 🔗 |
| 11 | sports.espn.go.com/espn/fp/pollDataJS | 1 | 🔗 |
| 12 | static.espn.go.com/swf/fp/superheadline.swf?h=Spur-fect+Ending&tex | 1 | 🔗 |
| 13 | espn.go.com | 1 | 🔗 |
| 14 | wimbledon.org/includes/js/external_sb.js | 1 | 🔗 |
| 15 | espn.go.com/swf/header2005/headers/mlb_hdr.swf | 1 | 🔗 |
| 16 | espn.go.com/swf/header2005/search/searchBar.swf | 1 | 🔗 |
| 17 | sports.espn.go.com/mlb/xml/upcomingTV?sport=mlb | 1 | 🔗 |
| 18 | espn.go.com/insertfiles/javascript/horizNav.js | 1 | 🔗 |
| 19 | sports.espn.go.com/mlb/index | 1 | 🔗 |
| 20 | espn.go.com/swf/header2005/tvschedule/tvschedule.swf | 1 | 🔗 |
| 21 | espn-i.starwave.com/media/apphoto/WATW11606230650_thumbnail.jpeg | 1 | 🔗 |
| 22 | espn.starwave.com/insertfiles/javascript/motion/motion_index_02.js | 1 | 🔗 |
| 23 | sports.espn.go.com/espn/fp/pollDataGen?id=30688 | 1 | 🔗 |

## 13.3 Web Site Submission

You may find that a web site has not been accurately categorized or that a web site's contents have changed and the content filtering category needs to be updated. Use the following procedure to submit the web site for review.

1. Log into the content filtering reports web site (see Section 13.2 on page 245).
2. In the **Web Filter Home** screen (see Figure 163 on page 248), click **Site Submissions** to open the **Web Page Review Process** screen shown next.

**Figure 167** Web Page Review Process Screen



Content Control from Blue Coat
Web Page Review Process
Please enter a valid site for the review process
Submit
Copyright © 2004, Blue Coat Systems, Inc. All rights reserved.
Next Generation Web Filtering

3 Type the web site's URL in the field and click **Submit** to have the web site reviewed.

# 14

# IPSec VPN

This chapter explains how to set up and maintain IPSec VPNs in the ZyWALL. First, it provides an overview of IPSec VPNs. Then, it introduces each screen for IPSec VPN in the ZyWALL.

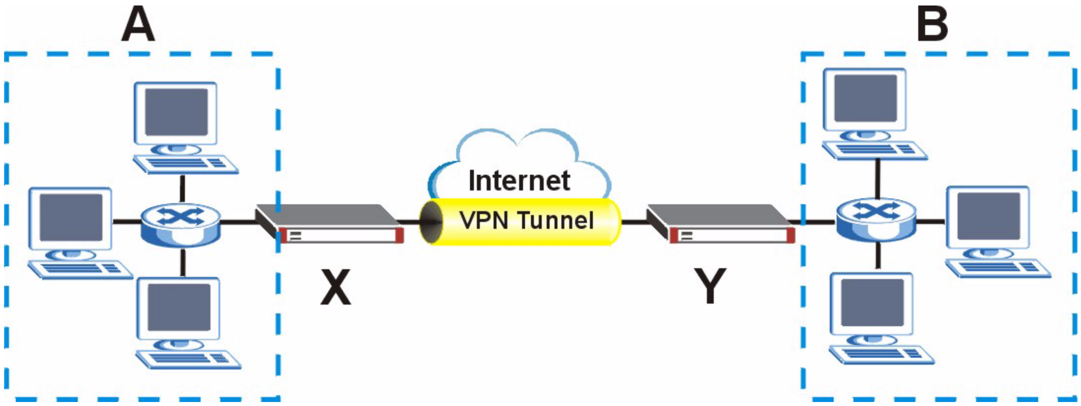
## 14.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure provides one perspective of a VPN tunnel.

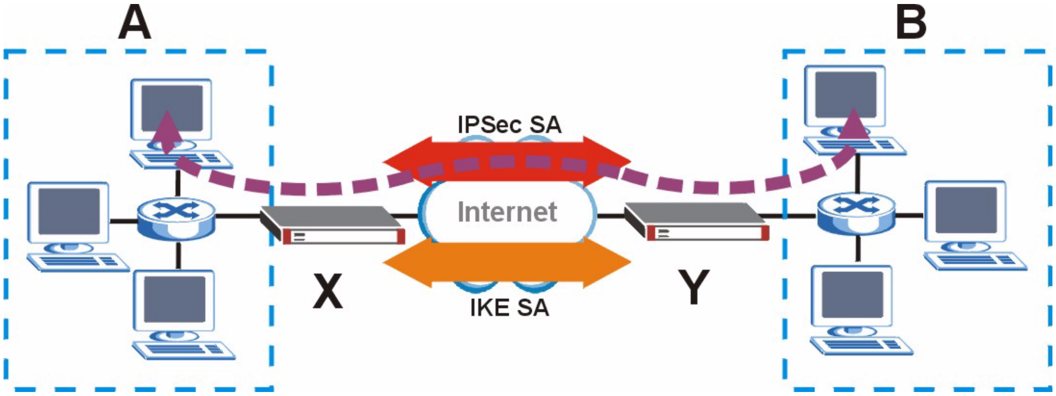
**Figure 168** VPN: Example



The VPN tunnel connects the ZyWALL (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyWALL and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

**Figure 169** VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

The rest of this section discusses IKE SA and IPSec SA in more detail.

## 14.1.1 IKE SA Overview

The IKE SA provides a secure connection between the ZyWALL and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines the number of steps to use. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Both routers must use the same negotiation mode.

These modes are discussed in more detail in Section 14.3.1.4 on page 260. Main mode is used in various examples in the rest of this section.

### 14.1.1.1 IP Addresses of the ZyWALL and Remote IPSec Router

In the ZyWALL, you have to specify the IP addresses of the ZyWALL and the remote IPSec router to establish an IKE SA.

You can usually provide a static IP address or a domain name for the ZyWALL. Sometimes, your ZyWALL might also offer another alternative, such as using the IP address of a port or interface.

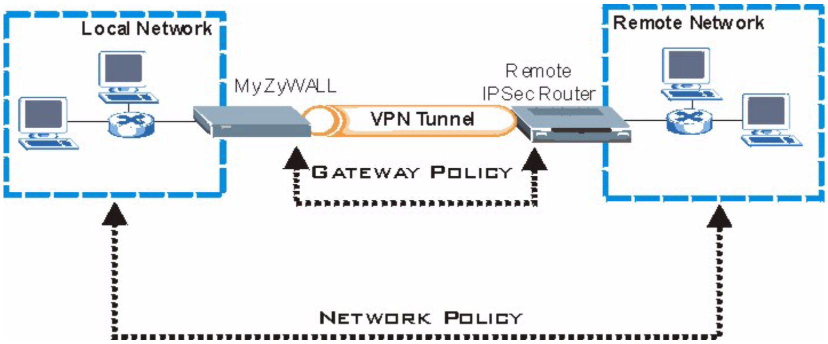
You can usually provide a static IP address or a domain name for the remote IPSec router as well. Sometimes, you might not know the IP address of the remote IPSec router (for example, telecommuters). In this case, you can still set up the IKE SA, but only the remote IPSec router can initiate an IKE SA.

## 14.2 VPN Rules (IKE)

A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.

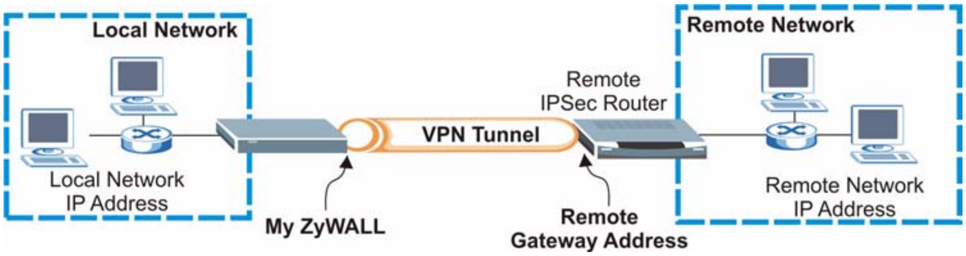
- A gateway policy contains the IKE SA settings. It identifies the IPSec routers at either end of a VPN tunnel.
- A network policy contains the IPSec SA settings. It specifies which devices (behind the IPSec routers) can use the VPN tunnel.

**Figure 170** Gateway and Network Policies


Local Network
Remote Network
MyZyWALL
Remote
IPSec Router
VPN Tunnel
GATEWAY POLICY
NETWORK POLICY

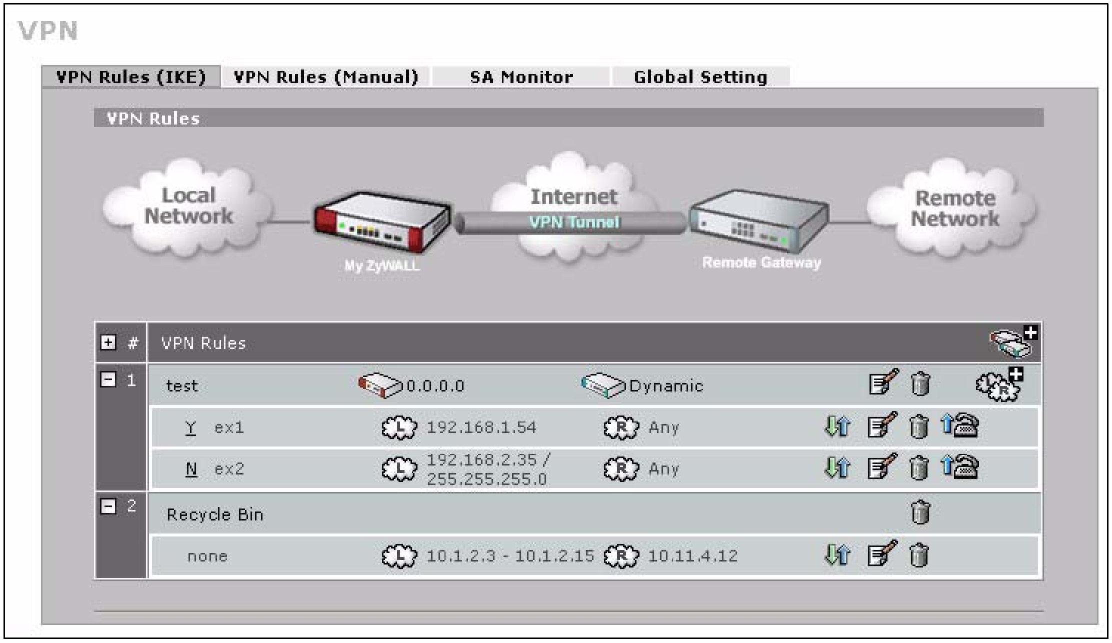
This figure helps explain the main fields in the VPN setup.

**Figure 171** IPSec Fields Summary


Local Network
Remote Network
Remote
IPSec Router
VPN Tunnel
Local Network
IP Address
My ZyWALL
Remote
Gateway Address
Remote Network
IP Address

Click **SECURITY** > **VPN** to display the **VPN Rules (IKE)** screen. Use this screen to manage the ZyWALL’s list of VPN rules (tunnels) that use IKE SAs.

**Figure 172** SECURITY > VPN > VPN Rules (IKE)



| # | VPN Rules | | |
|---|---|---|---|
| 1 | test | 0.0.0.0 | Dynamic |
| | Y ex1 | 192.168.1.54 | Any |
| | N ex2 | 192.168.2.35 / 255.255.255.0 | Any |
| 2 | Recycle Bin | | |
| | none | 10.1.2.3 - 10.1.2.15 | 10.11.4.12 |

The following table describes the labels in this screen.

**Table 64** SECURITY > VPN > VPN Rules (IKE)

| LABEL | DESCRIPTION |
|---|---|
| VPN Rules | These VPN rules define the settings for creating VPN tunnels for secure connection to other computers or networks. |
| | Click this icon to add a VPN gateway policy (or IPSec rule). |
| Gateway Policies | The first row of each VPN rule represents the gateway policy.<br>The gateway policy identifies the IPSec routers at either end of a VPN tunnel (**My ZyWALL** and **Remote Gateway**) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA (click the edit icon to display the other settings). |
| My ZyWALL | This represents your ZyWALL.<br>The WAN IP address, domain name or dynamic domain name of your ZyWALL displays in router mode.<br>The ZyWALL's IP address displays in bridge mode. |
| Remote Gateway | This represents the remote secure gateway.<br>The IP address, domain name or dynamic domain name of the remote IPSec router displays if you specify it, otherwise **Dynamic** displays. |
| | Click this icon to add a VPN network policy. |
| Network Policies | The subsequent rows in a VPN rule are network policies. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA. |
| Local Network | This is the network behind the ZyWALL. A network policy specifies which devices (behind the IPSec routers) can use the VPN tunnel. |
| Remote Network | This is the remote network behind the remote IPsec router. |
| | Click this icon to display a screen in which you can associate a network policy to a gateway policy or move it to the recycle bin. |

**Table 64** SECURITY > VPN > VPN Rules (IKE) (continued)

| LABEL | DESCRIPTION |
|---|---|
| ✎ | Click this icon to display a screen in which you can change the settings of a gateway or network policy. |
| 🗑 | Click this icon to delete a gateway or network policy. When you delete a gateway, the ZyWALL automatically moves the associated network policy(ies) to the recycle bin. When you delete a network policy, it is just deleted. |
| ⇧☎ | Click this icon to establish a VPN connection to a remote network. |
| ⇩☎ | Click this icon to drop a VPN connection to a remote network. |
| Y/N | This field displays whether a network policy is turned on (**Y**) or not (**N**). Click the letter to change it to the other state (click **Y** to change it to **N** or **N** to change it to **Y**). |
| Recycle Bin | The recycle bin appears when you have any network policies that are not associated to a gateway policy.<br>When you delete a gateway, the ZyWALL automatically moves the associated network policy(ies) to the recycle bin.<br>You can also manually move a network policy that you do not need (but may want to use again later) to the recycle bin. Click the network policy's move or edit icon and set it's **Gateway Policy** to **Recycle Bin**. |

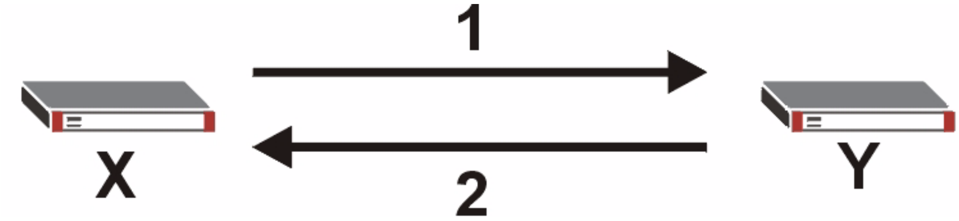
## 14.3 IKE SA Setup

This section provides more details about IKE SAs.

### 14.3.1 IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the ZyWALL and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated below.

**Figure 173** IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The ZyWALL sends one or more proposals to the remote IPSec router. (In some devices, you can set up only one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the ZyWALL wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the ZyWALL. If the remote IPSec router rejects all of the proposals (for example, if the VPN tunnel is not configured correctly), the ZyWALL and remote IPSec router cannot establish an IKE SA.

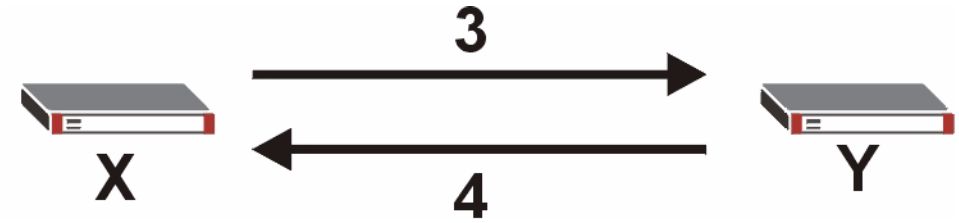
Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

See the field descriptions for information about specific encryption algorithms, authentication algorithms, and DH key groups. See Section 14.3.1.1 on page 258 for more information about DH key groups.

#### 14.3.1.1 Diffie-Hellman (DH) Key Exchange

The ZyWALL and the remote IPSec router use a DH key exchange to establish a shared secret, which is used to generate encryption keys for IKE SA and IPSec SA. In main mode, the DH key exchange is done in steps 3 and 4, as illustrated below.

**Figure 174** IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



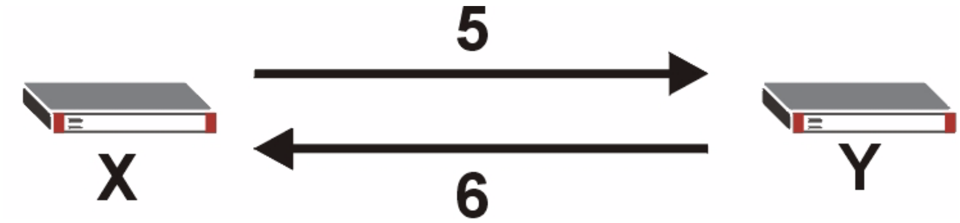
The DH key exchange is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption keys, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 encryption keys take longer to encrypt and decrypt.

#### 14.3.1.2 Authentication

Before the ZyWALL and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the ZyWALL and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. Their identities are encrypted using the encryption algorithm and encryption key the ZyWALL and remote IPSec router selected in previous steps.

**Figure 175** IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication



The ZyWALL and remote IPSec router use a pre-shared key in the authentication process, though it is not actually transmitted or exchanged.

The ZyWALL and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and ID content. The ID type can be IP address, domain name, or e-mail address, and the ID content is a specific IP address, domain name, or e-mail address. The ID content is only used for identification; the IP address, domain name, or e-mail address that you enter does not have to actually exist.

The ZyWALL and the remote IPSec router each has its own identity, so each one must store two sets of information, one for itself and one for the other router. Local ID type and ID content refers to the ID type and ID content that applies to the router itself, and peer ID type and ID content refers to the ID type and ID content that applies to the other router in the IKE SA.

The ZyWALL's local and peer ID type and ID content must match the remote IPSec router's peer and local ID type and ID content, respectively.

In the following example, the ID type and content match so the ZyWALL and the remote IPSec router authenticate each other successfully.

**Table 65** VPN Example: Matching ID Type and Content

| ZYWALL | REMOTE IPSEC ROUTER |
|---|---|
| Local ID type: E-mail | Local ID type: IP |
| Local ID content: tom@yourcompany.com | Local ID content: 1.1.1.2 |
| Peer ID type: IP | Peer ID type: E-mail |
| Peer ID content: 1.1.1.2 | Peer ID content: tom@yourcompany.com |

In the following example, the ID type and content do not match so the authentication fails and the ZyWALL and the remote IPSec router cannot establish an IKE SA.

**Table 66** VPN Example: Mismatching ID Type and Content

| ZYWALL | REMOTE IPSEC ROUTER |
|---|---|
| Local ID type: E-mail | Local ID type: IP |
| Local ID content: tom@yourcompany.com | Local ID content: **1.1.1.2** |
| Peer ID type: IP | Peer ID type: E-mail |
| Peer ID content: **1.1.1.15** | Peer ID content: tom@yourcompany.com |

It is also possible to configure the ZyWALL to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to **Any**. This is not as secure as other peer ID types, however.

#### *14.3.1.2.1 Certificates*

It is also possible for the ZyWALL and remote IPSec router to authenticate each other with certificates. In this case, the authentication process is different.

- Instead of using the pre-shared key, the ZyWALL and remote IPSec router check each other's certificates.
- The local ID type and ID content come from the certificate. On the ZyWALL, you simply select which certificate to use.
- If you set the peer ID type to **Any**, the ZyWALL authenticates the remote IPSec router using the trusted certificates and trusted CAs you have set up. Alternatively, if you want to use a specific certificate to authenticate the remote IPSec router, you can use the information in the certificate to specify the peer ID type and ID content.

You must set up the certificates for the ZyWALL and remote IPSec router before you can use certificates in IKE SA. See Chapter 15 on page 295 for more information about certificates.

#### 14.3.1.3 Extended Authentication

Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters. Extended authentication occurs right after the authentication described in Section 14.3.1.2 on page 258.

In extended authentication, one of the routers (the ZyWALL or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the ZyWALL to provide a user name and password to the remote IPSec router, or you can set up the ZyWALL to check a user name and password that is provided by the remote IPSec router.

#### 14.3.1.4 Negotiation Mode

There are two negotiation modes: main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1-2: The ZyWALL sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the ZyWALL.

Steps 3-4: The ZyWALL and the remote IPSec router participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

Steps 5-6: Finally, the ZyWALL and the remote IPSec router generate an encryption key from the shared secret, encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA.

Step 1: The ZyWALL sends its proposals to the remote IPSec router. It also starts the Diffie-Hellman key exchange and sends its (unencrypted) identity to the remote IPSec router for authentication.

Step 2: The remote IPSec router selects an acceptable proposal and sends it back to the ZyWALL. It also finishes the Diffie-Hellman key exchange, authenticates the ZyWALL, and sends its (unencrypted) identity to the ZyWALL for authentication.

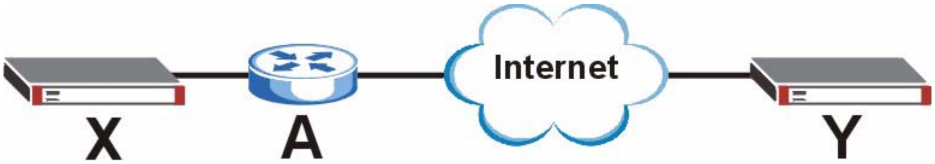
Step 3: The ZyWALL authenticates the remote IPSec router and confirms that the IKE SA is established.

Aggressive mode does not provide as much security as main mode because the identity of the ZyWALL and the identity of the remote IPSec router are not encrypted. It is usually used when the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication (for example, telecommuters).

#### 14.3.1.5 VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

**Figure 176** VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-through feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See Section 14.6.3 on page 272 for more information about active protocols.)

If router A does not have an IPSec pass-through or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the ZyWALL and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the ZyWALL and remote IPSec router support.

## 14.4 Additional IPSec VPN Topics

This section discusses other IPSec VPN topics that apply to either IKE SAs or IPSec SAs or both. Relationships between the topics are also highlighted.

### 14.4.1 SA Life Time

SAs have a lifetime that specifies how long the SA lasts until it times out. When an SA times out, the ZyWALL automatically renegotiates the SA in the following situations:

- There is traffic when the SA life time expires
- The IPSec SA is configured on the ZyWALL as nailed up (see below)

Otherwise, the ZyWALL must re-negotiate the SA the next time someone wants to send traffic.

If the IKE SA times out while an IPSec SA is connected, the IPSec SA stays connected.

An IPSec SA can be set to **nailed up**. Normally, the ZyWALL drops the IPSec SA when the life time expires or after two minutes of outbound traffic with no inbound traffic. If you set the IPSec SA to nailed up, the ZyWALL automatically renegotiates the IPSec SA when the SA life time expires, and it does not drop the IPSec SA if there is no inbound traffic.

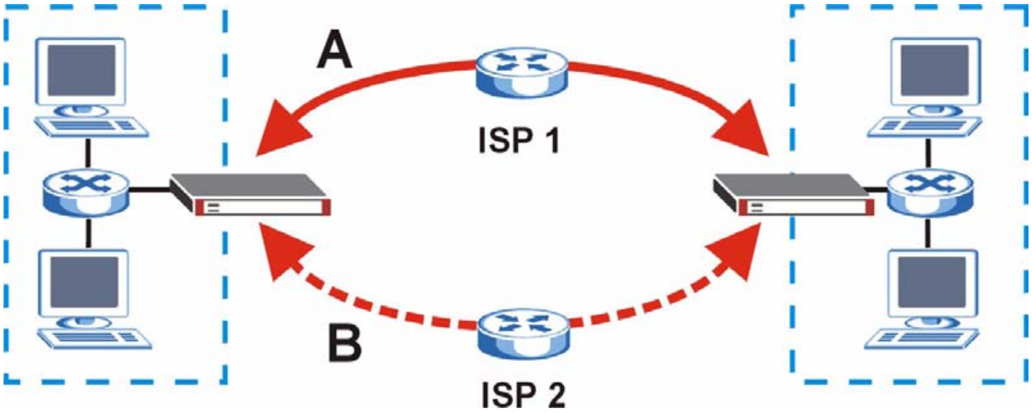
The SA life time and nailed up settings only apply if the rule identifies the remote IPSec router by a static IP address or a domain name. If the **Primary Remote Gateway** field is set to **0.0.0.0**, the ZyWALL cannot initiate the tunnel (and cannot renegotiate the SA).

### 14.4.2 IPSec High Availability

IPSec high availability (also known as VPN high availability) allows you to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down.

In the following figure, if the primary VPN tunnel (**A**) goes down, the ZyWALL uses the redundant VPN tunnel (**B**).

**Figure 177** IPSec High Availability



When setting up an IPSec high availability VPN tunnel, the remote IPSec router:

- Must have multiple WAN connections
- Only needs one corresponding IPSec rule
- Should only have IPSec high availability settings in its corresponding IPSec rule if your ZyWALL has multiple WAN connections
- Should ideally identify itself by a domain name or dynamic domain name (it must otherwise have **My Address** set to 0.0.0.0)
- Should use a WAN connectivity check to this ZyWALL's WAN IP address

If the remote IPSec router is not a ZyWALL, you may also want to avoid setting the IPSec rule to nailed up.

## 14.4.3 Encryption and Authentication Algorithms

In most ZyWALLs, you can select one of the following encryption algorithms for each proposal. The encryption algorithms are listed here in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.
- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Use the commands to have the AES encryption apply 192-bit or 256-bit keys to 128-bit blocks of data.

You can select one of the following authentication algorithms for each proposal. The algorithms are listed here in order from weakest to strongest.

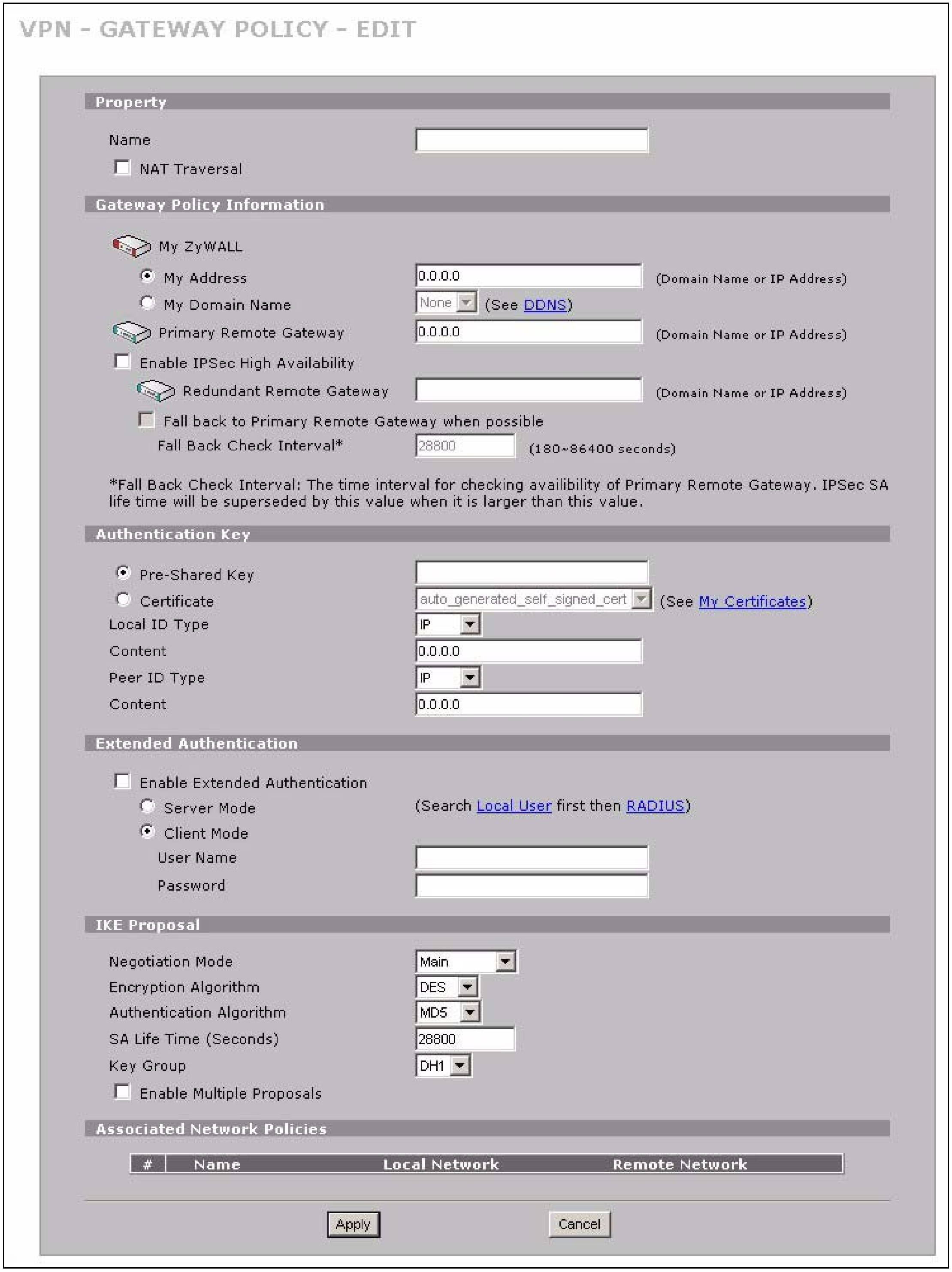
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

## 14.5 VPN Rules (IKE) Gateway Policy Edit

In the **VPN Rule (IKE)** screen, click the add gateway policy ( ) icon or the edit ( ) icon to display the **VPN-Gateway Policy -Edit** screen.

Use this screen to configure a VPN gateway policy. The gateway policy identifies the IPSec routers at either end of a VPN tunnel (**My ZyWALL** and **Remote Gateway**) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

**Figure 178** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy



VPN - GATEWAY POLICY - EDIT

**Property**

Name

☐ NAT Traversal

**Gateway Policy Information**

My ZyWALL

● My Address: 0.0.0.0 (Domain Name or IP Address)

○ My Domain Name: None (See DDNS)

Primary Remote Gateway: 0.0.0.0 (Domain Name or IP Address)

☐ Enable IPSec High Availability

Redundant Remote Gateway: (Domain Name or IP Address)

☐ Fall back to Primary Remote Gateway when possible

Fall Back Check Interval*: 28800 (180~86400 seconds)

*Fall Back Check Interval: The time interval for checking availibility of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.

**Authentication Key**

● Pre-Shared Key

○ Certificate: auto_generated_self_signed_cert (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: IP

Content: 0.0.0.0

**Extended Authentication**

☐ Enable Extended Authentication

○ Server Mode (Search Local User first then RADIUS)

● Client Mode

User Name

Password

**IKE Proposal**

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

SA Life Time (Seconds): 28800

Key Group: DH1

☐ Enable Multiple Proposals

**Associated Network Policies**

| # | Name | Local Network | Remote Network |
|---|---|---|---|

The following table describes the labels in this screen.

**Table 67** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy

| LABEL | DESCRIPTION |
|---|---|
| Property | |
| Name | Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| NAT Traversal | Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.<br>Note: The remote IPSec router must also have NAT traversal enabled. See Section 14.3.1.5 on page 261 for more information.<br>You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP ports 500 and 4500 to the IPSec router behind the NAT router. |
| Gateway Policy Information | |
| My ZyWALL | When the ZyWALL is in router mode, this field identifies the WAN IP address or domain name of the ZyWALL. You can select **My Address** and enter the ZyWALL's static WAN IP address (if it has one) or leave the field set to 0.0.0.0.<br>The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.<br>Otherwise, you can select **My Domain Name** and choose one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the ZyWALL use that dynamic domain name's IP address.<br>When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address.<br>The VPN tunnel has to be rebuilt if the **My ZyWALL** IP address changes after setup. |
| Primary Remote Gateway | Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address.<br>In order to have more than one active rule with the **Primary Remote Gateway** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules.<br>If you configure an active rule with **0.0.0.0** in the **Primary Remote Gateway** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Primary Remote Gateway** field set to **0.0.0.0**. |
| Enable IPSec High Availability | Turn on the high availability feature to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down. The remote IPSec router must have a second WAN connection in order for you to use this.<br>To use this, you must identify both the primary and the redundant remote IPSec routers by WAN IP address or domain name (you cannot set either to **0.0.0.0**). |
| Redundant Remote Gateway | Type the WAN IP address or the domain name (up to 31 characters) of the backup IPSec router to use when the ZyWALL cannot connect to the primary remote gateway. |

**Table 67** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Fall back to Primary Remote Gateway when possible | Select this to have the ZyWALL change back to using the primary remote gateway if the connection becomes available again. |
| Fall Back Check Interval* | Set how often the ZyWALL should check the connection to the primary remote gateway while connected to the redundant remote gateway.<br>Each gateway policy uses one or more network policies. If the fall back check interval is shorter than a network policy's SA life time, the fall back check interval is used as the check interval and network policy SA life time. If the fall back check interval is longer than a network policy's SA life time, the SA lifetime is used as the check interval and network policy SA life time. |
| Authentication Key | |
| Pre-Shared Key | Select the **Pre-Shared Key** radio button and type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.<br>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself.<br>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends. |
| Certificate | Select the **Certificate** radio button to identify the ZyWALL by a certificate.<br>Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen. Click **My Certificates** to go to the **My Certificates** screen where you can view the ZyWALL's list of certificates. |
| Local ID Type | Select **IP** to identify this ZyWALL by its IP address.<br>Select **DNS** to identify this ZyWALL by a domain name.<br>Select **E-mail** to identify this ZyWALL by an e-mail address.<br>You do not configure the local ID type and content when you set **Authentication Key** to **Certificate**. The ZyWALL takes them from the certificate you select. |
| Content | When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The ZyWALL automatically uses the IP address in the **My ZyWALL** field (refer to the **My** ZyWALL field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank.<br>It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations.<br>1. When there is a NAT router between the two IPSec routers.<br>2. When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.<br>When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyWALL in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. |

**Table 67** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Peer ID Type | Select from the following when you set **Authentication Key** to **Pre-shared Key**.<br>Select **IP** to identify the remote IPSec router by its IP address.<br>Select **DNS** to identify the remote IPSec router by a domain name.<br>Select **E-mail** to identify the remote IPSec router by an e-mail address.<br>Select from the following when you set **Authentication Key** to **Certificate**.<br>Select **IP** to identify the remote IPSec router by the IP address in the subject alternative name field of the certificate it uses for this VPN connection.<br>Select **DNS** to identify the remote IPSec router by the domain name in the subject alternative name field of the certificate it uses for this VPN connection.<br>Select **E-mail** to identify the remote IPSec router by the e-mail address in the subject alternative name field of the certificate it uses for this VPN connection.<br>Select **Subject Name** to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection.<br>Select **Any** to have the ZyWALL not check the remote IPSec router's ID. |
| Content | The configuration of the peer content depends on the peer ID type.<br>Do the following when you set **Authentication Key** to **Pre-shared Key**.<br>For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Primary Remote Gateway** field (refer to the **Primary Remote Gateway** field description).<br>For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.<br>It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations:<br>1. When there is a NAT router between the two IPSec routers.<br>2. When you want the ZyWALL to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.<br>Do the following when you set **Authentication Key** to **Certificate**.<br>1. For **IP**, type the IP address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Primary Remote Gateway** field (refer to the **Primary Remote Gateway** field description).<br>2. For **DNS** or **E-mail**, type the domain name or e-mail address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection.<br>3. For **Subject Name**, type the subject name of the certificate the remote IPSec router will use for this VPN connection. Use up to255 ASCII characters including spaces.<br>4. For **Any**, the peer **Content** field is not available.<br>5. Regardless of how you configure the **ID Type** and **Content** fields, two active IPSec SAs cannot have both the local and remote IP address ranges overlap between rules. |
| Extended Authentication | |
| Enable Extended Authentication | Select this check box to activate extended authentication. |

**Table 67** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Server Mode | Select **Server Mode** to have this ZyWALL authenticate extended authentication clients that request this VPN connection.<br>You must also configure the extended authentication clients' usernames and passwords in the authentication server's local user database or a RADIUS server (see Chapter 16 on page 323).<br>Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of user names and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server.<br>During authentication, if the ZyWALL (in server mode) does not find the extended authentication clients' user name in its internal user database and an external RADIUS server has been enabled, it attempts to authenticate the client through the RADIUS server. |
| Client Mode | Select **Client Mode** to have your ZyWALL use a username and password when initiating this VPN connection to the extended authentication server ZyWALL. Only a VPN extended authentication client can initiate this VPN connection. |
| User Name | Enter a user name for your ZyWALL to be authenticated by the VPN peer (in server mode). The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. You must enter a user name and password when you select client mode. |
| Password | Enter the corresponding password for the above user name. The password can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. |
| IKE Proposal | |
| Negotiation Mode | Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode. |
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>DES - a 56-bit key with the DES encryption algorithm<br>3DES - a 168-bit key with the DES encryption algorithm<br>AES - a 128-bit key with the AES encryption algorithm<br>The ZyWALL and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower. |
| SA Life Time (Seconds) | Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days).<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Key Group | Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are:<br>**DH1** - use a 768-bit random number<br>**DH2** - use a 1024-bit random number |
| Enable Multiple Proposals | Select this to allow the ZyWALL to use any of its phase 1 key groups and encryption and authentication algorithms when negotiating an IKE SA.<br>When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which phase 1 key groups and encryption and authentication algorithms to use for the IKE SA, even if they are less secure than the ones you configure for the VPN rule.<br>Clear this to have the ZyWALL use only the configured phase 1 key groups and encryption and authentication algorithms when negotiating an IKE SA. |

**Table 67** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Associated Network Policies | The following table shows the policy(ies) you configure for this rule.<br>To add a VPN policy, click the add network policy ( ) icon in the **VPN Rules (IKE)** screen (see Figure 172 on page 256). Refer to Section 14.8 on page 278 for more information. |
| # | This field displays the policy index number. |
| Name | This field displays the policy name. |
| Local Network | This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL. |
| Remote Network | This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 14.6 IPSec SA Overview

Once the ZyWALL and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

### 14.6.1 Local Network and Remote Network

In an IPSec SA, the local network consists of devices connected to the ZyWALL and may be called the local policy. Similarly, the remote network consists of the devices connected to the remote IPSec router and may be called the remote policy.

You can configure a remote network as 0.0.0.0 (any) when:

- Forwarding all outgoing traffic to the remote gateway.
- The remote network's addresses are unknown or there are many remote networks using one VPN rule (see Section 14.15.1 on page 289 for an example of telecommuters sharing one VPN rule).

It is not recommended to set a VPN rule’s local and remote network settings both to 0.0.0.0 (any).

In most cases you should use virtual address mapping (see Section 14.6.2 on page 271) to avoid overlapping local and remote network IP addresses. See Section 14.14 on page 286 for how the ZyWALL handles overlapping local and remote network IP addresses.

## 14.6.2 Virtual Address Mapping

Virtual address mapping (NAT over IPSec) changes the source IP addresses of packets from your local devices to virtual IP addresses before sending them through the VPN tunnel.

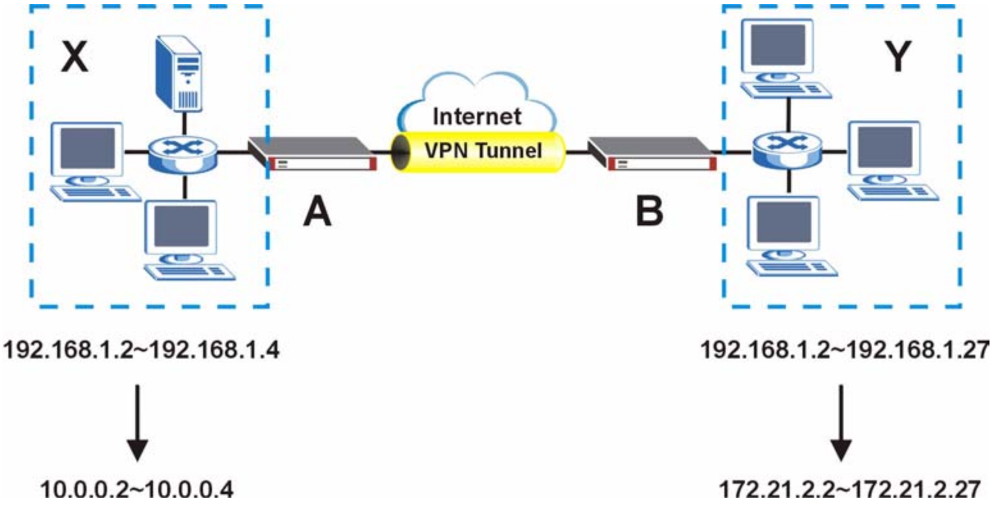
### 14.6.2.1 Avoiding Overlapping Local And Remote Network IP Addresses

If both IPSec routers support virtual address mapping, you can access devices on both networks, even if their IP addresses overlap. You map the ZyWALL's local network addresses to virtual IP addresses and map the remote IPSec router's local IP addresses to other (non-overlapping) virtual IP addresses.

The following diagram shows an example of using virutal address mapping to avoid overlapping local and remote IP addresses. You can set up virtual address mapping on both IPSec routers to allow computers on network **X** to access network **X** and network **Y** computers with the same IP address.

- You set ZyWALL **A** to change the source IP addresses of packets from local network **X** (192.168.1.2 to 192.168.1.4) to virtual IP addresses 10.0.0.2 to 10.0.0.4 before sending them through the VPN tunnel.
- You set ZyWALL **B** to change the source IP addresses of packets from the remote network **Y** (192.168.1.2 to 192.168.1.27) to virtual IP addresses 172.21.2.2 to 172.21.2.27 before sending them through the VPN tunnel.
- On ZyWALL **A**, you specify 172.21.2.2 to 172.21.2.27 as the remote network. On ZyWALL **B**, you specify 10.0.0.2 to 10.0.0.4 as the remote network.

**Figure 179** Virtual Mapping of Local and Remote Network IP Addresses



Computers on network **X** use IP addresses 192.168.1.2 to 192.168.1.4 to access local network devices and IP addresses 172.21.2.2 to 172.21.2.27 to access the remote network devices.

Computers on network **Y** use IP addresses 192.168.1.2 to 192.168.1.27 to access local network devices and IP addresses 10.0.0.2 to 10.0.0.4 to access the remote network devices.

### 14.6.3 Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

The ZyWALL and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

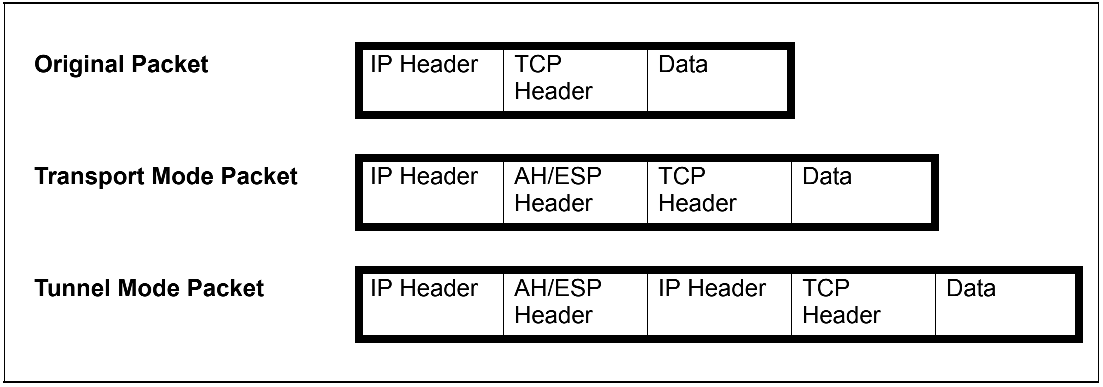
### 14.6.4 Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the ZyWALL and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

The ZyWALL and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

**Figure 180** VPN: Transport and Tunnel Mode Encapsulation


Original Packet
IP Header
TCP Header
Data
Transport Mode Packet
IP Header
AH/ESP Header
TCP Header
Data
Tunnel Mode Packet
IP Header
AH/ESP Header
IP Header
TCP Header
Data

In tunnel mode, the ZyWALL uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the ZyWALL or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the ZyWALL or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the ZyWALL includes part of the original IP header when it encapsulates the packet. With ESP, however, the ZyWALL does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

### 14.6.5 IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see Section 14.3.1 on page 257), except that you also have the choice whether or not the ZyWALL and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the ZyWALL and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

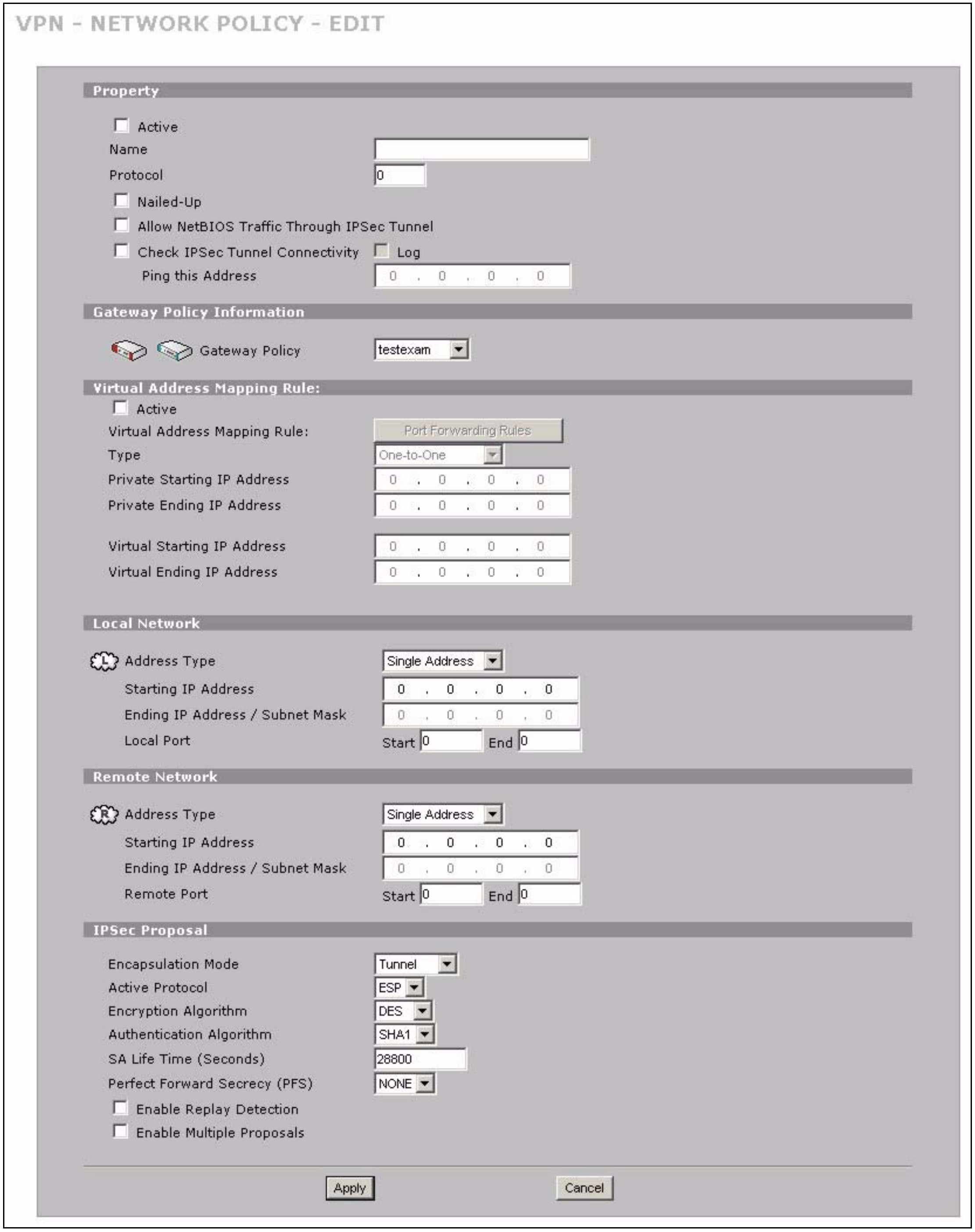
If you do not enable PFS, the ZyWALL and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

## 14.7 VPN Rules (IKE) Network Policy Edit

Click **SECURITY > VPN** and the add network policy (⚙) icon or a network policy's edit icon in the **VPN Rules (IKE)** screen to display the **VPN-Network Policy -Edit** screen. Use this screen to configure a network policy. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

**Figure 181** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy



VPN - NETWORK POLICY - EDIT

**Property**

☐ Active
Name:
Protocol: 0
☐ Nailed-Up
☐ Allow NetBIOS Traffic Through IPSec Tunnel
☐ Check IPSec Tunnel Connectivity ☐ Log
Ping this Address: 0 . 0 . 0 . 0

**Gateway Policy Information**

Gateway Policy: testexam

**Virtual Address Mapping Rule:**

☐ Active
Virtual Address Mapping Rule: Port Forwarding Rules
Type: One-to-One
Private Starting IP Address: 0 . 0 . 0 . 0
Private Ending IP Address: 0 . 0 . 0 . 0
Virtual Starting IP Address: 0 . 0 . 0 . 0
Virtual Ending IP Address: 0 . 0 . 0 . 0

**Local Network**

Address Type: Single Address
Starting IP Address: 0 . 0 . 0 . 0
Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0
Local Port: Start 0 End 0

**Remote Network**

Address Type: Single Address
Starting IP Address: 0 . 0 . 0 . 0
Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0
Remote Port: Start 0 End 0

**IPSec Proposal**

Encapsulation Mode: Tunnel
Active Protocol: ESP
Encryption Algorithm: DES
Authentication Algorithm: SHA1
SA Life Time (Seconds): 28800
Perfect Forward Secrecy (PFS): NONE
☐ Enable Replay Detection
☐ Enable Multiple Proposals

Apply Cancel

The following table describes the labels in this screen.

**Table 68** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy

| LABEL | DESCRIPTION |
|---|---|
| Active | If the **Active** check box is selected, packets for the tunnel trigger the ZyWALL to build the tunnel.<br>Clear the **Active** check box to turn the network policy off. The ZyWALL does not apply the policy. Packets for the tunnel do not trigger the tunnel.<br>If you clear the **Active** check box while the tunnel is up (and click **Apply**), you turn off the network policy and the tunnel goes down. |
| Name | Type a name to identify this VPN network policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Protocol | Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol. |
| Nailed-Up | Select this check box to turn on the nailed up feature for this SA.<br>Turn on nailed up to have the ZyWALL automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The ZyWALL also reinitiates the SA when it restarts.<br>The ZyWALL also rebuilds the tunnel if it was disconnected due to the output or input idle timer. |
| Allow NetBIOS Traffic Through IPSec Tunnel | This field is not available when the ZyWALL is in bridge mode.<br>NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.<br>Select this check box to send NetBIOS packets through the VPN connection. |
| Check IPSec Tunnel Connectivity | Select the check box and configure an IP address in the **Ping this Address** field to have the ZyWALL periodically test the VPN tunnel to the remote IPSec router.<br>The ZyWALL pings the IP address every minute. The ZyWALL starts the IPSec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote IPSec router by the time the timeout period expires, the ZyWALL disconnects the VPN tunnel. |
| Log | Select this check box to set the ZyWALL to create logs when it cannot ping the remote device. |
| Ping this Address | If you select **Check IPSec Tunnel Connectivity**, enter the IP address of a computer at the remote IPSec network. The computer's IP address must be in this IP policy's remote range (see the **Remote Network** fields). |
| Gateway Policy Information | |
| Gateway Policy | Select the gateway policy with which to use the VPN policy or store it in the recycle bin (without an association to any gateway policy). |
| Virtual Address Mapping Rule | Virtual address mapping over VPN is available with the routing mode. |
| Active | Enable this feature to have the ZyWALL use virtual (translated) IP addresses for the local network for the VPN connection. You do not configure the **Local Network** fields when you enable virtual address mapping.<br>Virtual address mapping allows local and remote networks to have overlapping IP addresses. Virtual address mapping (NAT over IPSec) translates the source IP addresses of computers on your local network to other (virtual) IP addresses before sending the packets to the remote IPSec router. This translation hides the source IP addresses of computers in the local network. |

**Table 68** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port Forwarding Rules | If you are configuring a **Many-to-One** rule, click this button to go to a screen where you can configure port forwarding for your VPN tunnels. The VPN network policy port forwarding rules let the ZyWALL forward traffic coming in through the VPN tunnel to the appropriate IP address. |
| Type | Select **One-to-One** to translate a single (static) IP address on your LAN to a single virtual IP address.<br>Select **Many-to-One** to translate a range of (static) IP addresses on your LAN to a single virtual IP address. Many-to-one rules are for traffic going out from your LAN, through the VPN tunnel, to the remote network. Use port forwarding rules to allow incoming traffic from the remote network.<br>Select **Many One-to-One** to translate a range of (static) IP addresses on your LAN to a range of virtual IP addresses. |
| Private Starting IP Address | Specify the IP addresses of the devices behind the ZyWALL that can use the VPN tunnel.<br>When you select **One-to-One** in the **Type** field, enter the (static) IP address of a computer on the LAN behind your ZyWALL.<br>When you select **Many-to-One** or **Many One-to-One** in the **Type** field, enter the beginning (static) IP address in a range of computers on the LAN behind your ZyWALL. |
| Private Ending IP Address | When you select **Many-to-One** or **Many One-to-One** in the **Type** field, enter the ending (static) IP address in a range of computers on the LAN behind your ZyWALL. |
| Virtual Starting IP Address | Enter the (static) IP addresses that represent the translated private IP addresses. These must correspond to the remote IPSec router's configured remote IP addresses.<br>When you select **One-to-One** or **Many-to-One** in the **Type** field, enter an IP address as the translated IP address. Many-to-one rules are only for traffic going to the remote network. Use port forwarding rules to allow incoming traffic from the remote network.<br>When you select **Many One-to-One** in the **Type** field, enter the beginning IP address of a range of translated IP addresses. |
| Virtual Ending IP Address | When you select **Many One-to-One** in the **Type** field, enter the ending (static) IP address of a range of translated IP addresses.<br>The size of the private address range must be equal to the size of the translated virtual address range. |
| Local Network | Specify the IP addresses of the devices behind the ZyWALL that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. You do not configure the **Local Network** fields when you enable virtual address mapping.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL. |

**Table 68** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Ending IP Address/ Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL. |
| Local Port | 0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3. |
| Remote Network | Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router. |
| Ending IP Address/ Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router. |
| Remote Port | 0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3. |
| IPSec Proposal | |
| Encapsulation Mode | Select **Tunnel** mode or **Transport** mode. |
| Active Protocol | Select the security protocols used for an SA.<br>Both **AH** and **ESP** increase processing requirements and communications latency (delay). |
| Encryption Algorithm | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>**NULL** - no encryption key or algorithm<br>DES - a 56-bit key with the DES encryption algorithm<br>3DES - a 168-bit key with the DES encryption algorithm<br>AES - a 128-bit key with the AES encryption algorithm<br>The ZyWALL and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower. |

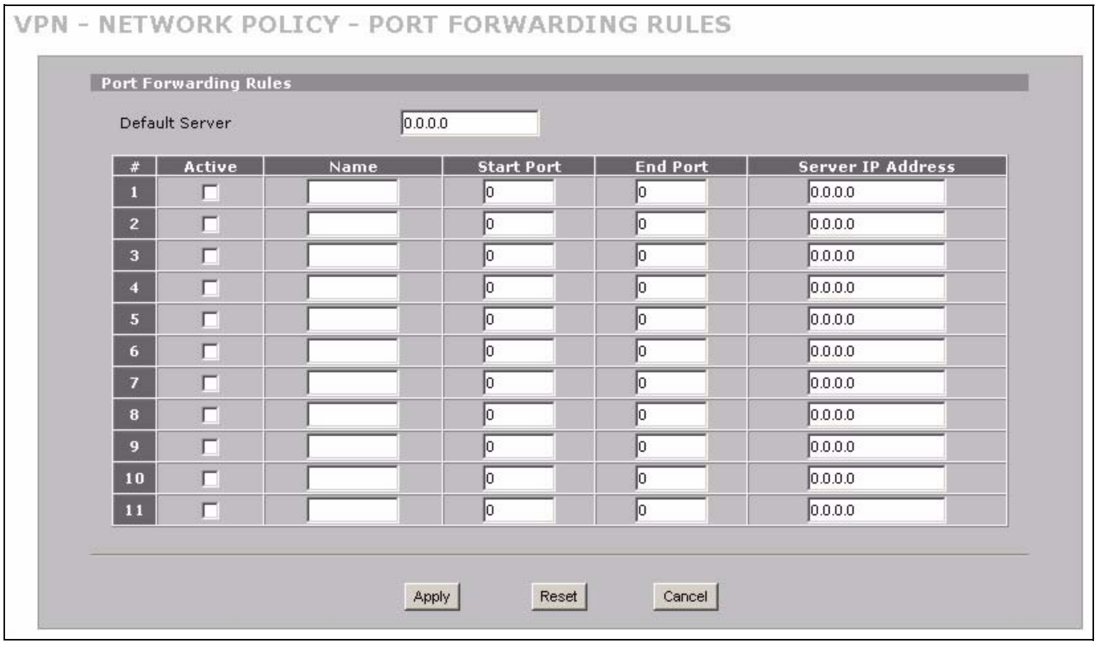
**Table 68** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| SA Life Time (Seconds) | Define the length of time before an IPSec SA automatically renegotiates in this field. The minimum value is 180 seconds.<br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Perfect Forward Secret (PFS) | Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are:<br>**NONE** - disable PFS<br>**DH1** - enable PFS and use a 768-bit random number<br>**DH2** - enable PFS and use a 1024-bit random number<br>PFS changes the root key that is used to generate encryption keys for each IPSec SA. It is more secure but takes more time. |
| Enable Replay Detection | As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box. |
| Enable Multiple Proposals | Select this to allow the ZyWALL to use any of its phase 2 encryption and authentication algorithms when negotiating an IPSec SA.<br>When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which phase 2 encryption and authentication algorithms to use for the IPSec SA, even if they are less secure than the ones you configure for the VPN rule.<br>Clear this to have the ZyWALL use only the configured phase 2 encryption and authentication algorithms when negotiating an IPSec SA. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard all changes and return to the main VPN screen. |

## 14.8 Network Policy Port Forwarding

Click **SECURITY** > **VPN** and the add network policy ( ) icon in the **VPN Rules (IKE)** screen to display the **VPN-Network Policy -Edit** screen. Then, under **Virtual Address Mapping Rule**, select **Many-to-One** as the **Type** and click the **Port Forwarding Rules** button to open the following screen. Use this screen to configure port forwarding for your VPN tunnels to let the ZyWALL forward traffic coming in through the VPN tunnel to the appropriate IP address on the LAN.

**Figure 182** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding



VPN - NETWORK POLICY - PORT FORWARDING RULES

Port Forwarding Rules

Default Server 0.0.0.0

| # | Active | Name | Start Port | End Port | Server IP Address |
|---|---|---|---|---|---|
| 1 | ☐ | | 0 | 0 | 0.0.0.0 |
| 2 | ☐ | | 0 | 0 | 0.0.0.0 |
| 3 | ☐ | | 0 | 0 | 0.0.0.0 |
| 4 | ☐ | | 0 | 0 | 0.0.0.0 |
| 5 | ☐ | | 0 | 0 | 0.0.0.0 |
| 6 | ☐ | | 0 | 0 | 0.0.0.0 |
| 7 | ☐ | | 0 | 0 | 0.0.0.0 |
| 8 | ☐ | | 0 | 0 | 0.0.0.0 |
| 9 | ☐ | | 0 | 0 | 0.0.0.0 |
| 10 | ☐ | | 0 | 0 | 0.0.0.0 |
| 11 | ☐ | | 0 | 0 | 0.0.0.0 |

The following table describes the labels in this screen.

**Table 69** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding

| LABEL | DESCRIPTION |
|---|---|
| Default Server | In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, all packets received for ports not specified in this screen are discarded. |
| # | Number of an individual port forwarding server entry. |
| Active | Select this check box to activate the port forwarding server entry. |
| Name | Enter a descriptive name for identifying purposes. |
| Start Port | Type a port number in this field.<br>To forward only one port, type the port number again in the **End Port** field.<br>To forward a series of ports, type the start port number here and the end port number in the **End Port** field. |
| End Port | Type a port number in this field.<br>To forward only one port, type the port number in the **Start Port** field above and then type it again in this field.<br>To forward a series of ports, type the last port number in a series that begins with the port number in the **Start Port** field above. |
| Server IP Address | Type your server IP address in this field. |
| Apply | Click this button to save these settings. |
| Reset | Click this button to begin configuring this screen afresh. |
| Cancel | Click this button to return to the **VPN-Network Policy -Edit** screen without saving your changes. |

## 14.9 Network Policy Move

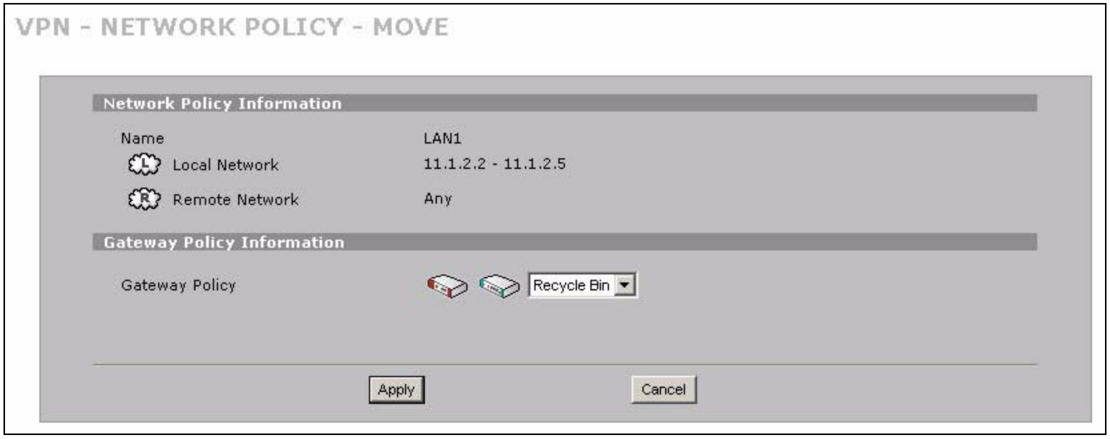
Click the move ( ⇅ ) icon in the **VPN Rules (IKE)** screen to display the **VPN Rules (IKE): Network Policy Move** screen.

A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network. Each VPN tunnel uses a single gateway policy and one or more network policies.

- The gateway policy contains the IKE SA settings. It identifies the IPSec routers at either end of a VPN tunnel.
- The network policy contains the IPSec SA settings. It specifies which devices (behind the IPSec routers) can use the VPN tunnel.

Use this screen to associate a network policy to a gateway policy.

**Figure 183** SECURITY > VPN > VPN Rules (IKE) > Move Network Policy


VPN - NETWORK POLICY - MOVE
Network Policy Information
Gateway Policy Information
Apply
Cancel

Name LAN1

Local Network 11.1.2.2 - 11.1.2.5

Remote Network Any

Gateway Policy Recycle Bin

The following table describes the labels in this screen.

**Table 70** SECURITY > VPN > VPN Rules (IKE) > Move Network Policy

| LABEL | DESCRIPTION |
|---|---|
| Network Policy Information | The following fields display the general network settings of this VPN policy. |
| Name | This field displays the policy name. |
| Local Network | This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL. |
| Remote Network | This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router. |
| Gateway Policy Information | |
| Gateway Policy | Select the name of a VPN rule (or gateway policy) to which you want to associate this VPN network policy.<br>If you do not want to associate a network policy to any gateway policy, select **Recycle Bin** from the drop-down list box. The **Recycle Bin** gateway policy is a virtual placeholder for any network policy(ies) without an associated gateway policy. When there is a network policy in **Recycle Bin**, the **Recycle Bin** gateway policy automatically displays in the **VPN Rules (IKE)** screen. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard all changes and return to the main VPN screen. |

# 14.10 IPSec SA Using Manual Keys

You might set up an IPSec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPSec SA.

In IPSec SAs using manual keys, the ZyWALL and remote IPSec router do not establish an IKE SA. They only establish an IPSec SA. As a result, an IPSec SA using manual keys has some characteristics of IKE SA and some characteristics of IPSec SA. There are also some differences between IPSec SA using manual keys and other types of SA.

## 14.10.1 IPSec SA Proposal Using Manual Keys

In IPSec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. You cannot specify several proposals. There is no DH key exchange, so you have to provide the encryption key and the authentication key the ZyWALL and remote IPSec router use.

The ZyWALL and remote IPSec router must use the same encryption key and authentication key.

## 14.10.2 Authentication and the Security Parameter Index (SPI)

For authentication, the ZyWALL and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

The ZyWALL and remote IPSec router must use the same SPI.

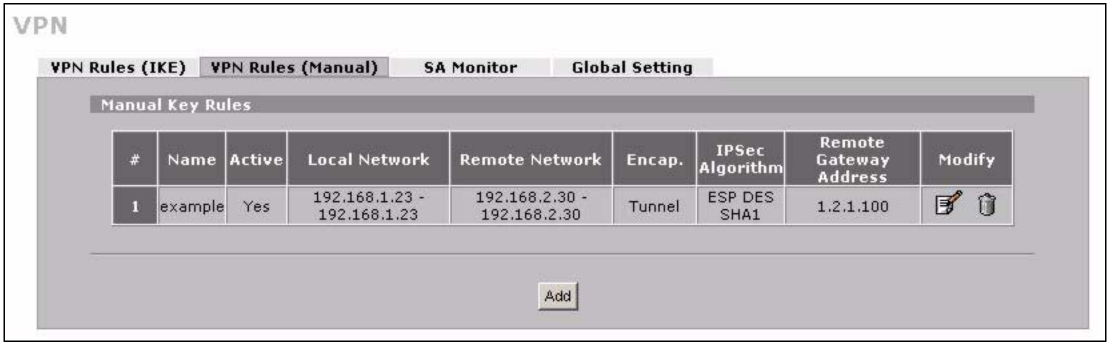
# 14.11 VPN Rules (Manual)

Refer to Figure 171 on page 255 for a graphical representation of the fields in the web configurator.

Click **SECURITY > VPN > VPN Rules (Manual)** to open the **VPN Rules (Manual)** screen.

Use this screen to manage the ZyWALL’s list of VPN rules (tunnels) that use manual keys. You may want to configure a VPN rule that uses manual key management if you are having problems with IKE key management.

**Figure 184** SECURITY > VPN > VPN Rules (Manual)



| # | Name | Active | Local Network | Remote Network | Encap. | IPSec Algorithm | Remote Gateway Address | Modify |
|---|---|---|---|---|---|---|---|---|
| 1 | example | Yes | 192.168.1.23 - 192.168.1.23 | 192.168.2.30 - 192.168.2.30 | Tunnel | ESP DES SHA1 | 1.2.1.100 | |

The following table describes the labels in this screen.

**Table 71** SECURITY > VPN > VPN Rules (Manual)

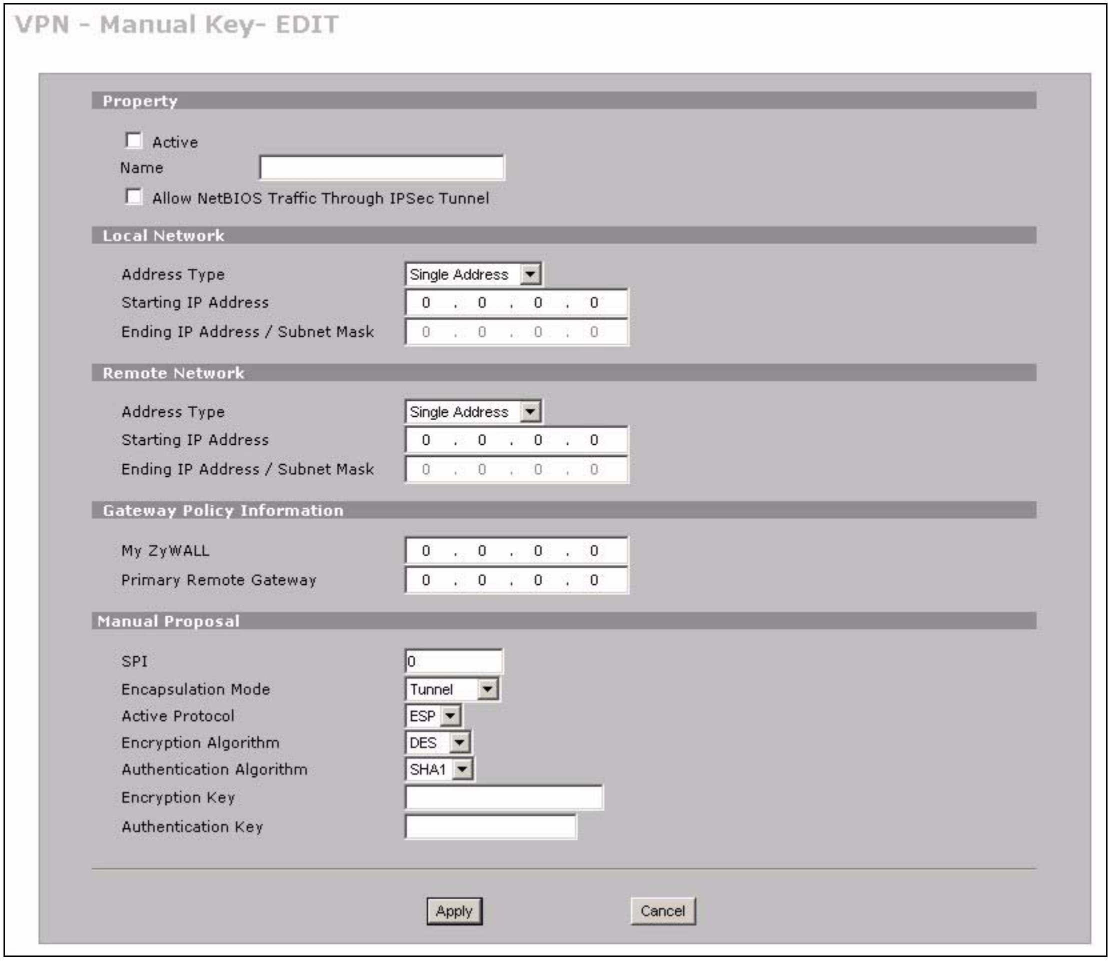
| LABEL | DESCRIPTION |
|---|---|
| # | This is the VPN policy index number. |
| Name | This field displays the identification name for this VPN policy. |
| Active | This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active. |
| Local Network | This is the IP address(es) of computer(s) on your local network behind your ZyWALL.<br>The same (static) IP address is displayed twice when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**.<br>The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**.<br>A (static) IP address and a subnet mask are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**. |
| Remote Network | This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router.<br>This field displays **N/A** when the **Remote Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.<br>The same (static) IP address is displayed twice when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**.<br>The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**.<br>A (static) IP address and a subnet mask are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**. |
| Encap. | This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection). |
| IPSec Algorithm | This field displays the security protocols used for an SA.<br>Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay). |
| Remote Gateway Address | This is the static WAN IP address of the remote IPSec router. |
| Modify | Click the edit icon to edit the VPN policy.<br>Click the delete icon to remove the VPN policy. A window displays asking you to confirm that you want to delete the VPN rule. When a VPN policy is deleted, subsequent policies move up in the page list. |
| Add | Click **Add** to add a new VPN policy. |

## 14.12 VPN Rules (Manual) Edit

Click the edit icon on the **VPN Rules (Manual)** screen to open the following screen. Use this screen to configure VPN rules that use manual keys. Manual key management is useful if you have problems with IKE key management.

See Section 14.10 on page 281 for more information about IPSec SAs using manual keys.

**Figure 185** SECURITY > VPN > VPN Rules (Manual) > Edit



VPN - Manual Key- EDIT

Property

☐ Active

Name:

☐ Allow NetBIOS Traffic Through IPSec Tunnel

Local Network

Address Type: Single Address

Starting IP Address: 0 . 0 . 0 . 0

Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0

Remote Network

Address Type: Single Address

Starting IP Address: 0 . 0 . 0 . 0

Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0

Gateway Policy Information

My ZyWALL: 0 . 0 . 0 . 0

Primary Remote Gateway: 0 . 0 . 0 . 0

Manual Proposal

SPI: 0

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

Encryption Key:

Authentication Key:

The following table describes the labels in this screen.

**Table 72** SECURITY > VPN > VPN Rules (Manual) > Edit

| LABEL | DESCRIPTION |
|---|---|
| Property | |
| Active | Select this check box to activate this VPN policy. |
| Name | Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Allow NetBIOS Traffic Through IPSec Tunnel | This field is not available when the ZyWALL is in bridge mode.<br>NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.<br>Select this check box to send NetBIOS packets through the VPN connection. |

**Table 72** SECURITY > VPN > VPN Rules (Manual) > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Local Network | Specify the IP addresses of the devices behind the ZyWALL that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL. |
| Ending IP Address/Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL. |
| Remote Network | Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router. |
| Ending IP Address/Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router. |
| Gateway Policy Information | |
| My ZyWALL | When the ZyWALL is in router mode, enter the WAN IP address of your ZyWALL or leave the field set to **0.0.0.0**.<br>The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.<br>The VPN tunnel has to be rebuilt if this IP address changes.<br>When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address. |

**Table 72** SECURITY > VPN > VPN Rules (Manual) > Edit (continued)

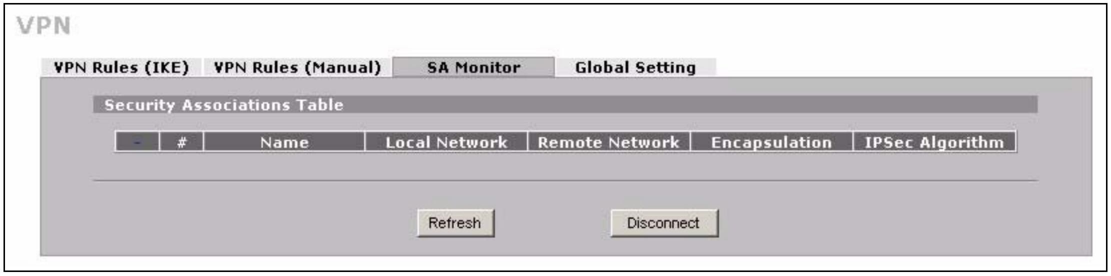
| LABEL | DESCRIPTION |
|---|---|
| Primary Remote Gateway | Type the WAN IP address of the IPSec router with which you're making the VPN connection. |
| Manual Proposal | |
| SPI | Type a unique **SPI** (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9". |
| Encapsulation Mode | Select **Tunnel** mode or **Transport** mode from the drop-down list box. |
| Active Protocol | Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).<br>Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described next). |
| Encryption Algorithm | Select **DES**, **3DES** or **NULL** from the drop-down list box.<br>When **DES** is used for data communications, both sender and receiver must know the **Encryption Key**, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key. |
| Authentication Algorithm | Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security. |
| Encryption Key | This field is applicable when you select **ESP** in the **Active Protocol** field above.<br>With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated. |
| Authentication Key | Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 14.13 VPN SA Monitor

In the web configurator, click **SECURITY > VPN > SA Monitor**. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections.

**Figure 186** SECURITY > VPN > SA Monitor



The following table describes the labels in this screen.

**Table 73** SECURITY > VPN > SA Monitor

| LABEL | DESCRIPTION |
|---|---|
| # | This is the security association index number. |
| Name | This field displays the identification name for this VPN policy. |
| Local Network | This field displays the IP address of the computer using the VPN IPSec feature of your ZyWALL. |
| Remote Network | This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router. |
| Encapsulation | This field displays **Tunnel** or **Transport** mode. |
| IPSec Algorithm | This field displays the security protocols used for an SA.<br>Both AH and ESP increase ZyWALL processing requirements and communications latency (delay). |
| Refresh | Click **Refresh** to display the current active VPN connection(s). |
| Disconnect | Select a security association index number that you want to disconnect and then click **Disconnect**. |

## 14.14 VPN Global Setting

Click **SECURITY** > **VPN** > **Global Setting** to open the **VPN Global Setting** screen. Use this screen to change settings that apply to all of your VPN tunnels.

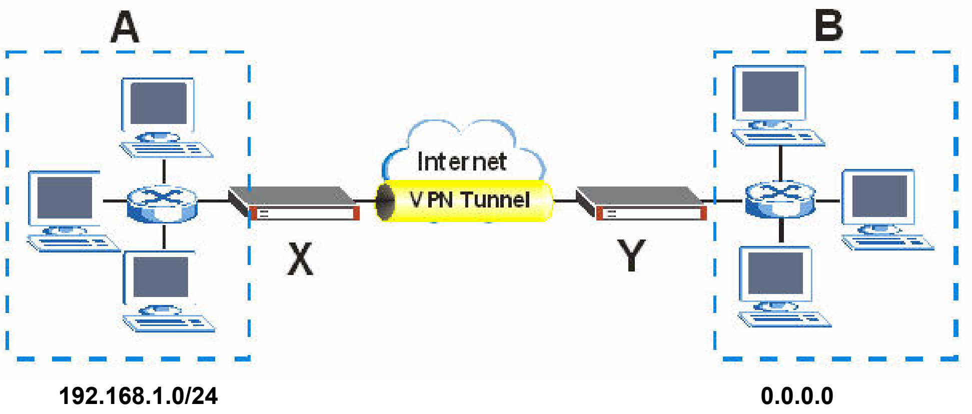
### 14.14.1 Local and Remote IP Address Conflict Resolution

Normally, you do not configure your local VPN policy rule's IP addresses to overlap with the remote VPN policy rule's IP addresses (see Section 14.6.2 on page 271). For example, you usually would not configure both with 192.168.1.0. However, overlapping local and remote network IP addresses can occur with dynamic VPN rules or IP alias.

#### 14.14.1.1 Dynamic VPN Rule

Local and remote network IP addresses can overlap when you configure a dynamic VPN rule for a remote site (see Figure 187). For example, when you configure ZyWALL **X**, you configure the local network as 192.168.1.0/24 and the remote network as any (0.0.0.0). The "any" includes all possible IP addresses. It will forward traffic from network **A** to network **B** even if both the sender (for example 192.168.1.8) and the receiver (for example 192.168.1.9) are in network **A**. Note that the remote access can still use the VPN tunnel to access computers on ZyWALL **X**'s network.

**Figure 187** Overlap in a Dynamic VPN Rule



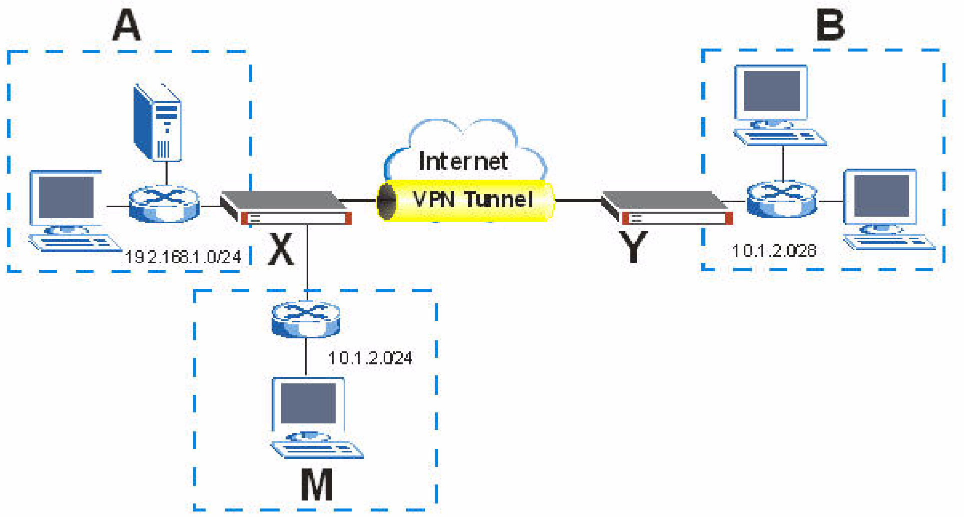
- Setting **Local and Remote IP Address Conflict Resolution** to **The Local Network** has the ZyWALL check if a packet's destination is also at the local network before forwarding the packet. If it is, the ZyWALL sends the traffic to the local network.
- Setting **Local and Remote IP Address Conflict Resolution** to **The Remote Network** disables the checking for local network IP addresses.

### 14.14.1.2 IP Alias

You could have an IP alias network that overlaps with the VPN remote network (see Figure 188). For example, you have an IP alias network **M** (10.1.2.0/24) in ZyWALL **X**'s LAN. For the VPN rule, you configure the VPN network as follows.

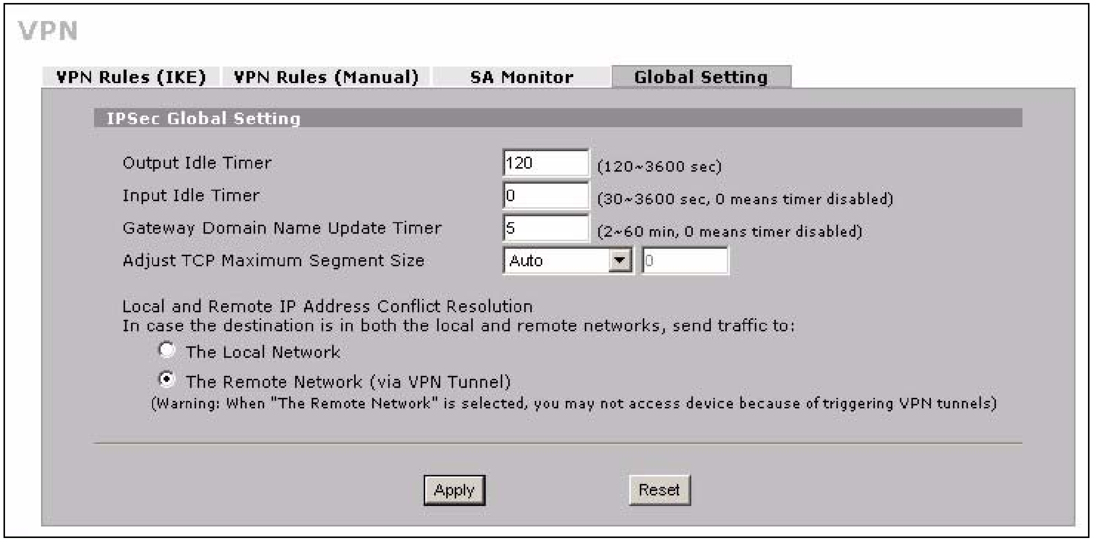
- Local IP address start: 192.168.1.1, end: 192.168.1.254
- Remote IP address start: 10.1.2.240, end: 10.1.2.254
- IP addresses 10.1.2.240 to 10.1.2.254 overlap.

**Figure 188** Overlap in IP Alias and VPN Remote Networks



In this case, if you want to send packets from network **A** to an overlapped IP (ex. 10.1.2.241) that is in the IP alias network **M**, you have to set **Local and Remote IP Address Conflict Resolution** to **The Local Network**.

**Figure 189** SECURITY > VPN > Global Setting



Output Idle Timer: 120 (120~3600 sec)

Input Idle Timer: 0 (30~3600 sec, 0 means timer disabled)

Gateway Domain Name Update Timer: 5 (2~60 min, 0 means timer disabled)

Adjust TCP Maximum Segment Size: Auto 0

Local and Remote IP Address Conflict Resolution
In case the destination is in both the local and remote networks, send traffic to:

○ The Local Network

● The Remote Network (via VPN Tunnel)

(Warning: When "The Remote Network" is selected, you may not access device because of triggering VPN tunnels)

The following table describes the labels in this screen.

**Table 74** SECURITY > VPN > Global Setting

| LABEL | DESCRIPTION |
|---|---|
| Output Idle Timer | The ZyWALL disconnects a VPN tunnel if the remote IPSec router does not reply for this number of seconds. |
| Input Idle Timer | When no traffic is received from a remote IPSec router after the specified time period, the ZyWALL disconnects the VPN tunnel. **0** disables the check (this is the default setting).<br>The output idle timer never takes effect if you set this timer to a shorter period. |
| Gateway Domain Name Update Timer | This field is applicable when you enter a domain name to identify the ZyWALL and/or the remote secure gateway.<br>Enter the time period (between 2 and 60 minutes) to wait before the ZyWALL updates the domain name and IP address mapping through a DNS server. The ZyWALL rebuilds the VPN tunnel if it finds that the domain name is now using a different IP address (any users of the VPN tunnel will be temporarily disconnected).<br>Enter **0** to disable this feature. |
| Adjust TCP Maximum Segment Size | The TCP packets are larger after the ZyWALL encrypts them for VPN. The ZyWALL fragments packets that are larger than a connection’s MTU (Maximum Transmit Unit).<br>In most cases you should leave this set to **Auto**. The ZyWALL automatically sets the Maximum Segment Size (MSS) of the TCP packets that are to be encrypted by VPN based on the encapsulation type.<br>Select **Off** to not adjust the MSS for the encrypted TCP packets.<br>If your network environment causes fragmentation issues that are affecting your throughput performance, you can manually set a smaller MSS for the TCP packets that are to be encrypted by VPN. Select **User-Defined** and specify a size from 0~1460 bytes. 0 has the ZyWALL use the auto setting. |

**Table 74** SECURITY > VPN > Global Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| Local and Remote IP Address Conflict Resolution | Select **The Local Network** to send packets destined for overlapping local and remote IP addresses to the local network (you can access the local devices but not the remote devices).<br>Select **The Remote Network (via VPN Tunnel)** to send packets destined for overlapping local and remote IP addresses to the remote network (you can access the remote devices but not the local devices.)<br>If the remote IPSec router also supports NAT over IPSec, it is recommended that you use NAT over IPSec (see Section 14.6.2 on page 271) if the local and remote IP addresses overlap.<br>If a VPN rule's local and remote network settings are both set to 0.0.0.0 (any), no traffic goes through the VPN tunnel if you select **The Local Network**. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 14.15 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyWALL at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The ZyWALL at headquarters has a static public IP address.

### 14.15.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a ZyWALL at headquarters (**HQ** in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

**Figure 190** Telecommuters Sharing One VPN Rule Example

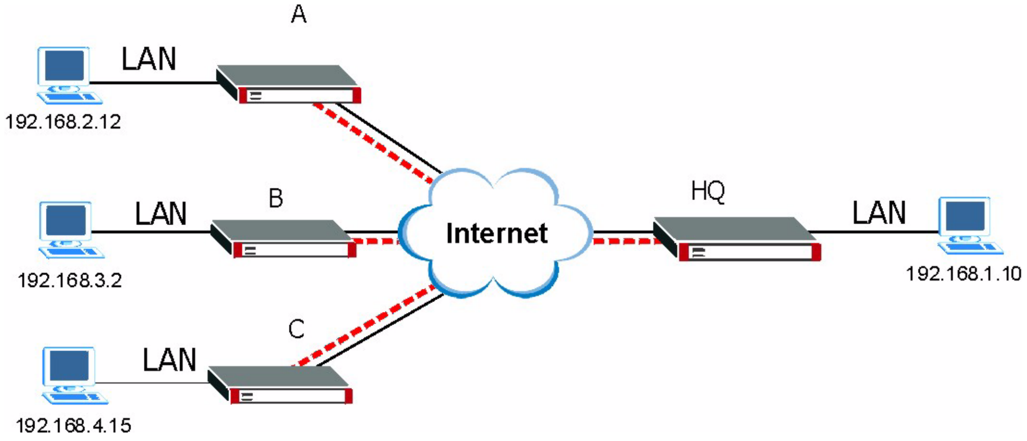


**Table 75** Telecommuters Sharing One VPN Rule Example

| FIELDS | TELECOMMUTERS | HEADQUARTERS |
|---|---|---|
| My ZyWALL: | 0.0.0.0 (dynamic IP address assigned by the ISP) | Public static IP address |
| Remote Gateway Address: | Public static IP address | 0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel. |
| Local Network - Single IP Address: | Telecommuter A: 192.168.2.12<br>Telecommuter B: 192.168.3.2<br>Telecommuter C: 192.168.4.15 | 192.168.1.10 |
| Remote Network - Single IP Address: | 192.168.1.10 | Not Applicable |

## 14.15.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see Section 14.3.1.4 on page 260), the ZyWALL can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyWALL at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyWALL at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a ZyWALL located at headquarters. The ZyWALL at headquarters (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The ZyWALL at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

**Figure 191** Telecommuters Using Unique VPN Rules Example

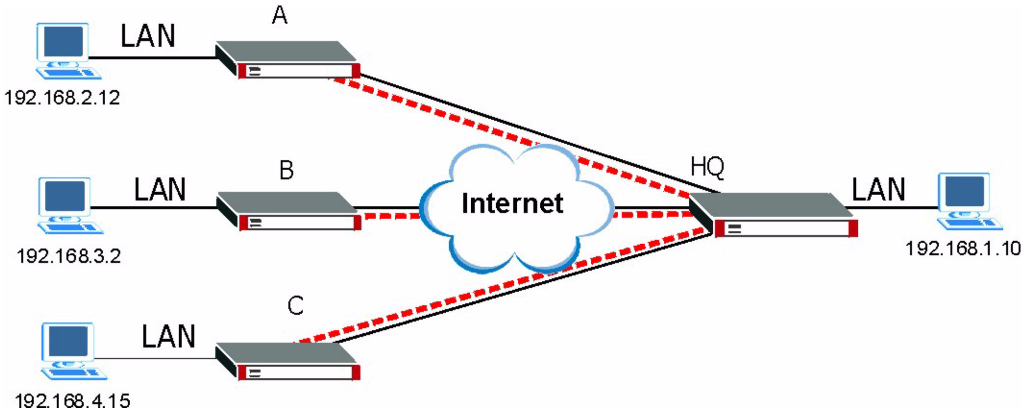


**Table 76** Telecommuters Using Unique VPN Rules Example

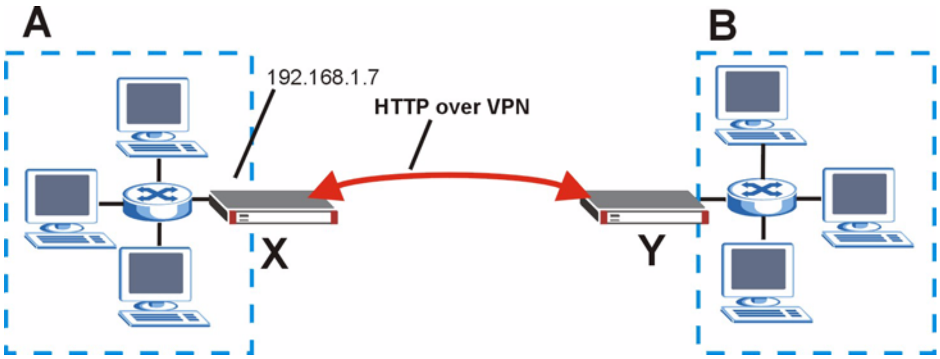
| TELECOMMUTERS | HEADQUARTERS |
|---|---|
| All Telecommuter Rules: | All Headquarters Rules: |
| My ZyWALL 0.0.0.0 | My ZyWALL: bigcompanyhq.com |
| Remote Gateway Address: bigcompanyhq.com | Local Network - Single IP Address: 192.168.1.10 |
| Remote Network - Single IP Address: 192.168.1.10 | Local ID Type: E-mail |
| Peer ID Type: E-mail | Local ID Content: bob@bigcompanyhq.com |
| Peer ID Content: bob@bigcompanyhq.com | |
| | |
| Telecommuter A (telecommutera.dydns.org) | Headquarters ZyWALL Rule 1: |
| Local ID Type: IP | Peer ID Type: IP |
| Local ID Content: 192.168.2.12 | Peer ID Content: 192.168.2.12 |
| Local IP Address: 192.168.2.12 | Remote Gateway Address: telecommutera.dydns.org |
| | Remote Address 192.168.2.12 |
| | |
| Telecommuter B (telecommuterb.dydns.org) | Headquarters ZyWALL Rule 2: |
| Local ID Type: DNS | Peer ID Type: DNS |
| Local ID Content: telecommuterb.com | Peer ID Content: telecommuterb.com |
| Local IP Address: 192.168.3.2 | Remote Gateway Address: telecommuterb.dydns.org |
| | Remote Address 192.168.3.2 |
| | |
| Telecommuter C (telecommuterc.dydns.org) | Headquarters ZyWALL Rule 3: |
| Local ID Type: E-mail | Peer ID Type: E-mail |
| Local ID Content: myVPN@myplace.com | Peer ID Content: myVPN@myplace.com |
| Local IP Address: 192.168.4.15 | Remote Gateway Address: telecommuterc.dydns.org |
| | Remote Address 192.168.4.15 |

## 14.16 VPN and Remote Management

You can allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the ZyWALL. One of the ZyWALL's ports must be part of the VPN rule's local network. This can be the ZyWALL's LAN port if you do not want to allow remote management on the WAN port. You also have to configure remote management (**REMOTE MGMT**) to allow management access for the service through the specific port.

In the following example, the VPN rule's local network (A) includes the ZyWALL's LAN IP address of 192.168.1.7. Someone in the remote network (B) can use a service (like HTTP for example) through the VPN tunnel to access the ZyWALL's LAN interface. Remote management must also be configured to allow HTTP access on the ZyWALL's LAN interface.

**Figure 192** VPN for Remote Management Example

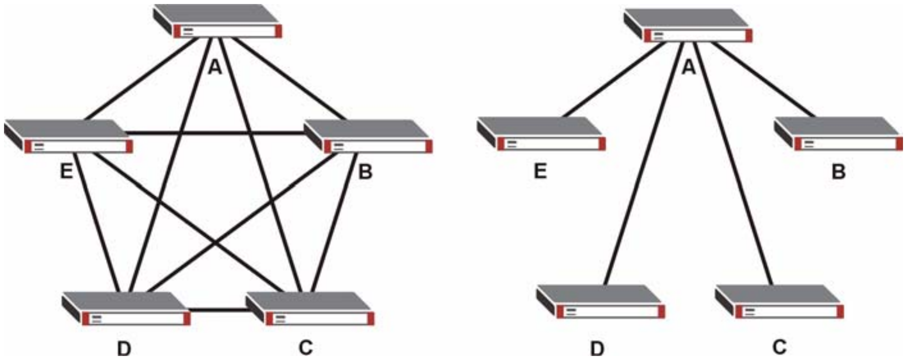


## 14.17 Hub-and-spoke VPN

Hub-and-spoke VPN connects VPN tunnels to form one secure network.

Figure 193 on page 292 shows some example network topologies. In the first (fully-meshed) approach, there is a VPN connection between every pair of routers. In the second (hub-and-spoke) approach, there is a VPN connection between each spoke router (**B**, **C**, **D**, and **E**) and the hub router (**A**). The hub router routes VPN traffic between the spoke routers and itself.

**Figure 193** VPN Topologies



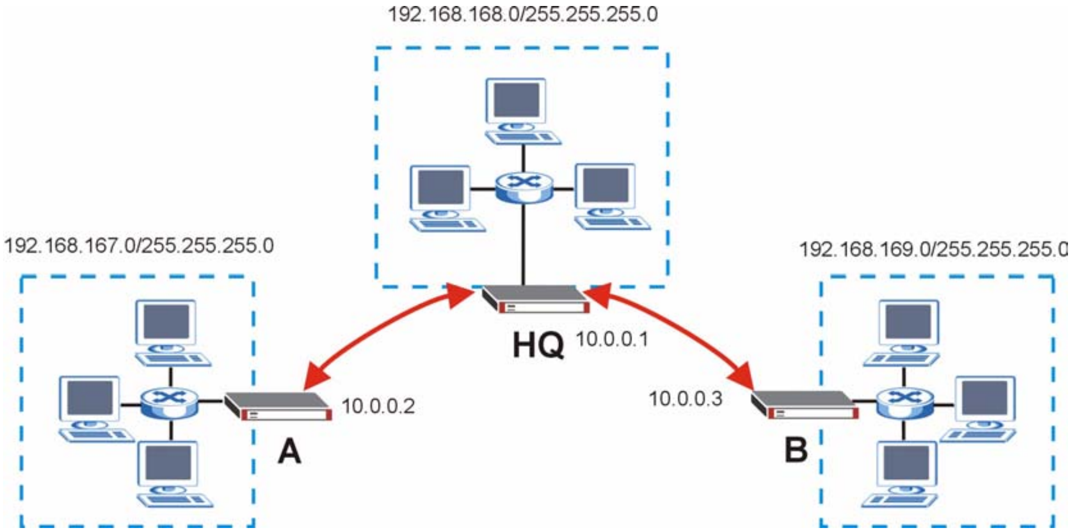
Hub-and-spoke VPN reduces the number of VPN connections that you have to set up and maintain in the network. Small office or telecommuter IPSec routers that support a limited number of VPN tunnels are also able to use VPN to connect to more networks. Hub-and-spoke VPN makes it easier for the hub router to manage the traffic between the spoke routers. If you have the spoke routers access the Internet through the hub-and-spoke VPN tunnel, the hub router can also provide content filtering protection for the spoke routers.

You should not use a hub-and-spoke VPN in every situation, however. The hub router is a single point of failure, so a hub-and-spoke VPN may not be appropriate if the connection between the spoke routers cannot be down occasionally (for maintenance, for example). In addition, there is a significant burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out where to send it, encrypts it, and sends it to the appropriate spoke. Therefore, a hub-and-spoke VPN is more suitable when there is a minimum amount of traffic between spoke routers.

### 14.17.1 Hub-and-spoke VPN Example

The following figure shows a basic hub-and-spoke VPN. Branch office A uses one VPN rule to access both the headquarters (HQ) network and branch office B's network. Branch office B uses one VPN rule to access both the headquarters and branch office A's networks.

**Figure 194** Hub-and-spoke VPN Example



### 14.17.2 Hub-and-spoke Example VPN Rule Addresses

The VPN rules for this hub-and-spoke example would use the following address settings.

Branch Office A:

- Remote Gateway: 10.0.0.1
- Local IP address: 192.168.167.0/255.255.255.0
- Remote IP address: 192.168.168.0~192.168.169.255

Headquarters:

Rule 1:

- Remote Gateway: 10.0.0.2
- Local IP address: 192.168.168.0~192.168.169.255
- Remote IP address:192.168.167.0/255.255.255.0

Rule 2:

- Remote Gateway: 10.0.0.3
- Local IP address: 192.168.167.0~192.168.168.255
- Remote IP address: 192.168.169.0/255.255.255.0

Branch Office B:

- Remote Gateway: 10.0.0.1
- Local IP address: 192.168.169.0/255.255.255.0
- Remote IP address: 192.168.167.0~192.168.168.255

### 14.17.3 Hub-and-spoke VPN Requirements and Suggestions

Consider the following when implementing a hub-and-spoke VPN.

The local IP addresses configured in the VPN rules cannot overlap

The hub router must have at least one separate VPN rule for each spoke. In the local IP address, specify the IP addresses of the hub-and-spoke networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule.

If you want to have the spoke routers access the Internet through the hub-and-spoke VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.

Make sure that your **From VPN** and **To VPN** firewall rules do not block the VPN packets.

# 15

# Certificates

This chapter gives background information about public-key certificates and explains how to use them.

## 15.1 Certificates Overview

The ZyWALL can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyWALL to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyWALL uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyWALL does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyWALL can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

### 15.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyWALL only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

## 15.2 Self-signed Certificates

You can have the ZyWALL act as a certification authority and sign its own certificates.

## 15.3 Verifying a Certificate

Before you import a trusted CA or trusted remote host certificate into the ZyWALL, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the ZyWALL also trusts any valid certificate signed by any of the imported trusted CA certificates.

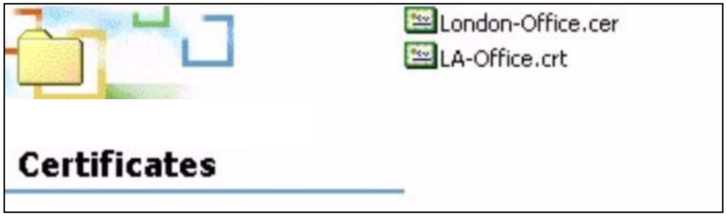
### 15.3.1 Checking the Fingerprint of a Certificate on Your Computer

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

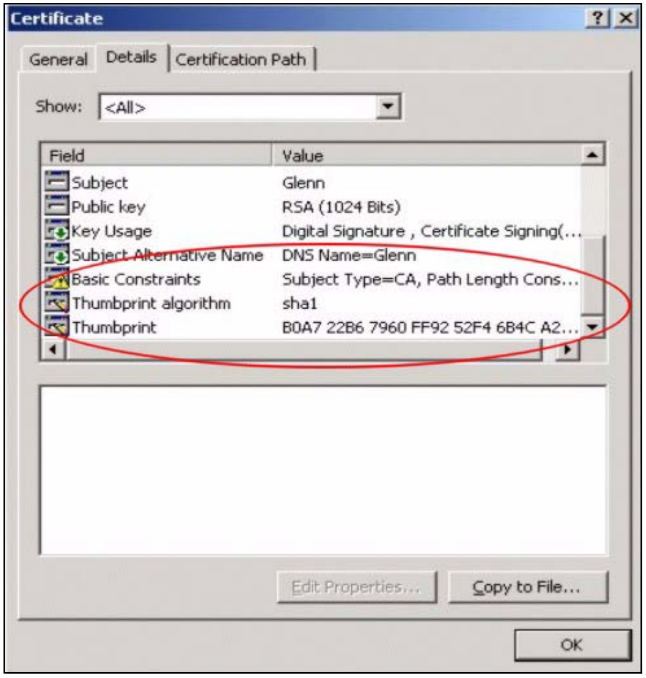
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 195** Certificates on Your Computer



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

**Figure 196** Certificate Details


Certificate
?
General
Details
Certification Path
Edit Properties...
Copy to File...
OK

Show: <All>

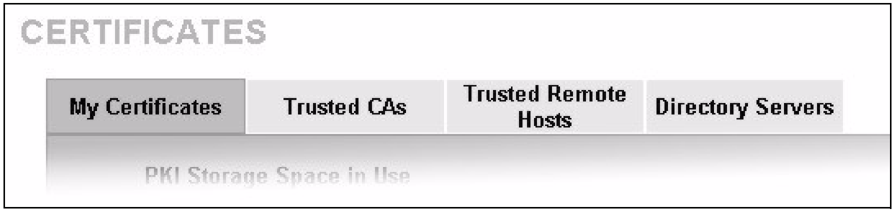
| Field | Value |
|---|---|
| Subject | Glenn |
| Public key | RSA (1024 Bits) |
| Key Usage | Digital Signature , Certificate Signing(... |
| Subject Alternative Name | DNS Name=Glenn |
| Basic Constraints | Subject Type=CA, Path Length Cons... |
| Thumbprint algorithm | sha1 |
| Thumbprint | B0A7 22B6 7960 FF92 52F4 6B4C A2... |

4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

## 15.4 Configuration Summary

This section summarizes how to manage certificates on the ZyWALL.

**Figure 197** Certificate Configuration Overview


CERTIFICATES
My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use

Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyWALL's CA-signed certificates.

Use the **Trusted CA** screens to save the certificates of trusted CAs to the ZyWALL. You can also export the certificates to a computer.

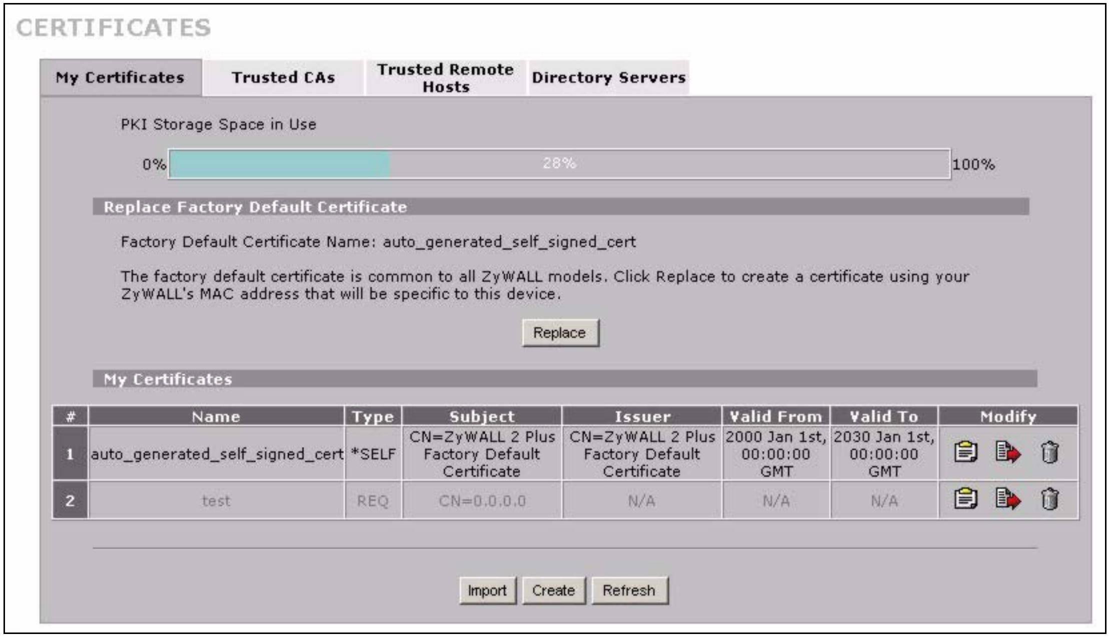
Use the **Trusted Remote Hosts** screens to import self-signed certificates from trusted remote hosts.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

## 15.5 My Certificates

Click **SECURITY** > **CERTIFICATES** > **My Certificates** to open the **My Certificates** screen. This is the ZyWALL’s summary list of certificates and certification requests. Certificates display in black and certification requests display in gray.

**Figure 198** SECURITY > CERTIFICATES > My Certificates



PKI Storage Space in Use

**Replace Factory Default Certificate**

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to all ZyWALL models. Click Replace to create a certificate using your ZyWALL's MAC address that will be specific to this device.

**My Certificates**

| # | Name | Type | Subject | Issuer | Valid From | Valid To | Modify |
|---|---|---|---|---|---|---|---|
| 1 | auto_generated_self_signed_cert | *SELF | CN=ZyWALL 2 Plus Factory Default Certificate | CN=ZyWALL 2 Plus Factory Default Certificate | 2000 Jan 1st, 00:00:00 GMT | 2030 Jan 1st, 00:00:00 GMT | |
| 2 | test | REQ | CN=0.0.0.0 | N/A | N/A | N/A | |

The following table describes the labels in this screen.

**Table 77** SECURITY > CERTIFICATES > My Certificates

| LABEL | DESCRIPTION |
|---|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyWALL’s PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| Replace | This button displays when the ZyWALL has the factory default certificate. The factory default certificate is common to all ZyWALLs that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyWALL's MAC address. |
| # | This field displays the certificate index number. The certificates are listed in alphabetical order. |
| Name | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. |
| Type | This field displays what kind of certificate this is.<br>**REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request.<br>**SELF** represents a self-signed certificate.<br>***SELF** represents the default self-signed certificate, which the ZyWALL uses to sign imported trusted remote host certificates.<br>**CERT** represents a certificate issued by a certification authority. |

**Table 77** SECURITY > CERTIFICATES > My Certificates (continued)

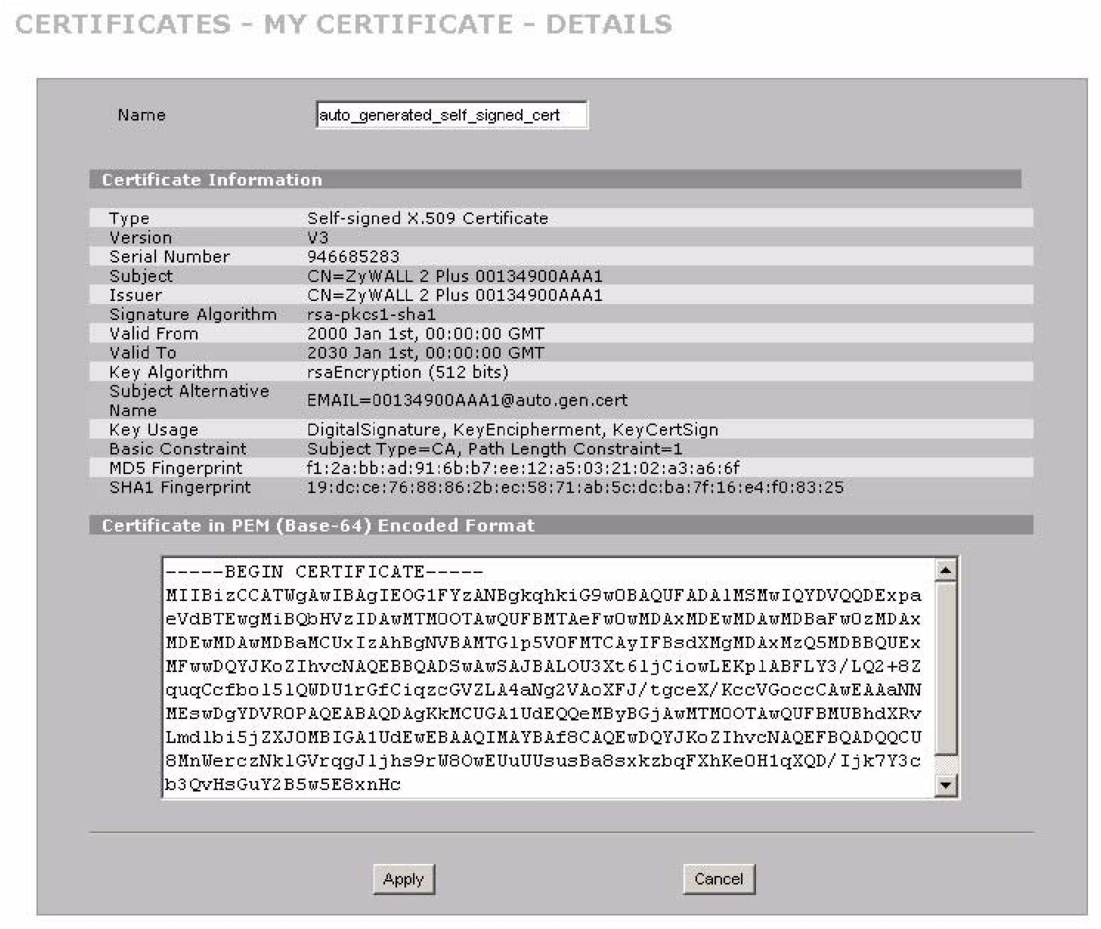
| LABEL | DESCRIPTION |
|---|---|
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field. |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Modify | Click the details icon to open a screen with an in-depth list of information about the certificate (or certification request).<br>Click the export icon to save the certificate to a computer. For a certification request, click the export icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.<br>Click the delete icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate.<br>You cannot delete a certificate that one or more features is configured to use.<br>Do the following to delete a certificate that shows ***SELF** in the **Type** field.<br>1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the ***SELF** certificate.<br>2. Click the details icon next to another self-signed certificate (see the description on the **Create** button if you need to create a self-signed certificate).<br>3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box.<br>4. Click **Apply** to save the changes and return to the **My Certificates** screen.<br>5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now.<br>Note that subsequent certificates move up by one when you take this action.<br>The poll now icon displays when the ZyWALL generates a certification request successfully but the CA does not issue a certificate and sends a pending notification to the ZyWALL. If the icon displays, you can manually click the icon to have the ZyWALL query the CA (or RA (Registration Authority)) server for a certificate immediately. Otherwise, the ZyWALL checks with the server and updates the status periodically. The poll now icon disappears after the ZyWALL gets a certificate or the request has failed permanently due to being rejected by the CA server. |
| Import | Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyWALL. |
| Create | Click **Create** to go to the screen where you can have the ZyWALL generate a certificate or a certification request. |
| Refresh | Click **Refresh** to display the current validity status of the certificates. |

## 15.6 My Certificate Details

Click **SECURITY** > **CERTIFICATES** > **My Certificates** to open the **My Certificates** screen (see Figure 198 on page 298). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

If it is a self-signed certificate, you can also set the ZyWALL to use the certificate to sign the imported trusted remote host certificates.

**Figure 199** SECURITY > CERTIFICATES > My Certificates > Details



Name: auto_generated_self_signed_cert

Certificate Information

| | |
|---|---|
| Type | Self-signed X.509 Certificate |
| Version | V3 |
| Serial Number | 946685283 |
| Subject | CN=ZyWALL 2 Plus 00134900AAA1 |
| Issuer | CN=ZyWALL 2 Plus 00134900AAA1 |
| Signature Algorithm | rsa-pkcs1-sha1 |
| Valid From | 2000 Jan 1st, 00:00:00 GMT |
| Valid To | 2030 Jan 1st, 00:00:00 GMT |
| Key Algorithm | rsaEncryption (512 bits) |
| Subject Alternative Name | EMAIL=00134900AAA1@auto.gen.cert |
| Key Usage | DigitalSignature, KeyEncipherment, KeyCertSign |
| Basic Constraint | Subject Type=CA, Path Length Constraint=1 |
| MD5 Fingerprint | f1:2a:bb:ad:91:6b:b7:ee:12:a5:03:21:02:a3:a6:6f |
| SHA1 Fingerprint | 19:dc:ce:76:88:86:2b:ec:58:71:ab:5c:dc:ba:7f:16:e4:f0:83:25 |

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN CERTIFICATE-----
MIIBizCCATWgAwIBAgIEOG1FYzANBgkqhkiG9w0BAQUFADA1MSMwIQYDVQQDExpa
eVdBTEwgMiBQbHVzIDAwMTM0OTAwQUFBMTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAx
MDEwMDAwMDBaMCUxIzAhBgNVBAMTGlp5V0FMTCAyIFBsdXMgMDAxMzQ5MDBBQUEx
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALOU3Xt6ljCiowLEKplABFLY3/LQ2+8Z
quqCcfbol5lQWDU1rGfCiqzcGVZLA4aNg2VAoXFJ/tgceX/KccVGoccCAwEAAaNN
MEswDgYDVR0PAQEABAQDAgKkMCUGA1UdEQQeMByBGjAwMTM0OTAwQUFBMUBhdXRv
Lmdlbi5jZXJ0MBIGA1UdEwEBAAQIMAYBAf8CAQEwDQYJKoZIhvcNAQEFBQADQQCU
8MnWerczNklGVrqgJljhs9rW8OwEUuUUsusBa8sxkzbqFXhKeOH1qXQD/Ijk7Y3c
b3QvHsGuY2B5w5E8xnHc
```

The following table describes the labels in this screen.

**Table 78** SECURITY > CERTIFICATES > My Certificates > Details

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces). |
| Certificate Information | These read-only fields display detailed information about the certificate. |

**Table 78** SECURITY > CERTIFICATES > My Certificates > Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| Type | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates. |
| Version | This field displays the X.509 version number. |
| Serial Number | This field displays the certificate's identification number given by the certification authority or generated by the ZyWALL. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br>With self-signed certificates, this is the same as the **Subject Name** field. |
| Signature Algorithm | This field displays the type of algorithm that was used to sign the certificate. The ZyWALL uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example). |
| Subject Alternative Name | This field displays the certificate owner‘s IP address (IP), domain name (DNS) or e-mail address (EMAIL). |
| Key Usage | This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text. |
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. |
| MD5 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. |
| SHA1 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.<br>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.<br>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |

**Table 78** SECURITY > CERTIFICATES > My Certificates > Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

## 15.7 My Certificate Export

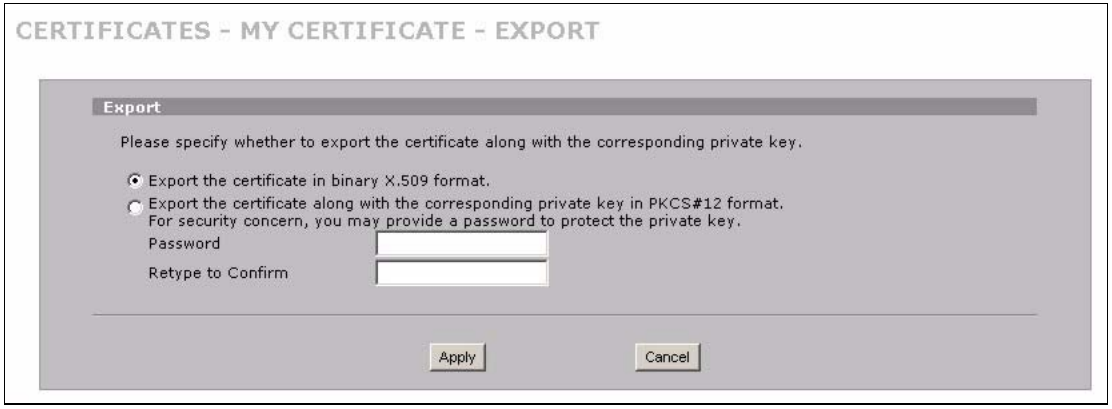
Click **SECURITY** > **CERTIFICATES** > **My Certificates** and then a certificate's export icon to open the **My Certificate Export** screen. Follow the instructions in this screen to choose the file format to use for saving the certificate from the ZyWALL to a computer.

### 15.7.1 Certificate File Export Formats

You can export a certificate in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ZyWALL.

**Figure 200** SECURITY > CERTIFICATES > My Certificates > Export



CERTIFICATES - MY CERTIFICATE - EXPORT

Export

Please specify whether to export the certificate along with the corresponding private key.

● Export the certificate in binary X.509 format.

○ Export the certificate along with the corresponding private key in PKCS#12 format.
For security concern, you may provide a password to protect the private key.

The following table describes the labels in this screen.

**Table 79** SECURITY > CERTIFICATES > My Certificates > Export

| LABEL | DESCRIPTION |
|---|---|
| Export the certificate in binary X.509 format. | Binary X.509 is an ITU-T recommendation that defines the formats for X.509 certificates. |
| Export the certificate along with the corresponding private key in PKCS#12 format. | PKCS#12 is a format for transferring public key and private key certificates. You can also password-encrypt the private key in the PKCS #12 file. The file's password is not connected to your certificate's public or private passwords. |
| Password | Type the file's password to use for encrypting the private key. The password is optional, although you must specify one if you want to be able to import the PKCS#12 format certificate into Netscape version 7.2. |
| Retype to confirm | Type the password to make sure that you have entered it correctly. |
| Apply | Click **Apply** and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

## 15.8 My Certificate Import

Click **SECURITY > CERTIFICATES > My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate from a computer to the ZyWALL.

- You can only import a certificate that matches a corresponding certification request that was generated by the ZyWALL (the certification request contains the private key). The certificate you import replaces the corresponding request in the My Certificates screen. One exception is that you can import a PKCS#12 format certificate without a corresponding certification request since the certificate includes the private key.
- You must remove any spaces from the certificate's filename before you can import it.

### 15.8.1 Certificate File Formats

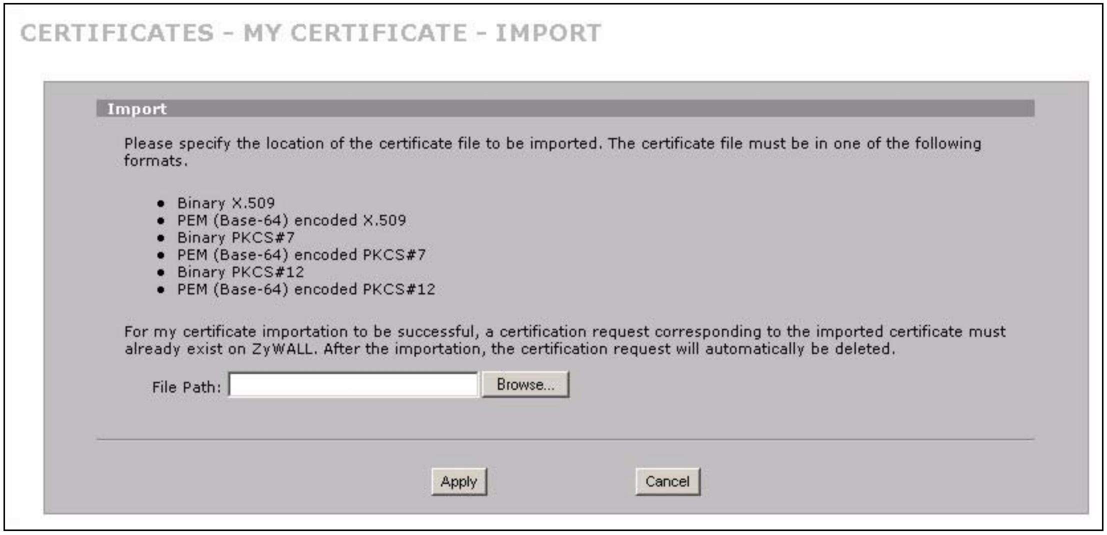
The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyWALL currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

- Binary PKCS#12: This is a format for transferring public key and private key certificates. The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ZyWALL.

Be careful to not convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

**Figure 201** SECURITY > CERTIFICATES > My Certificates > Import



CERTIFICATES - MY CERTIFICATE - IMPORT

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7
- Binary PKCS#12
- PEM (Base-64) encoded PKCS#12

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted.

File Path:

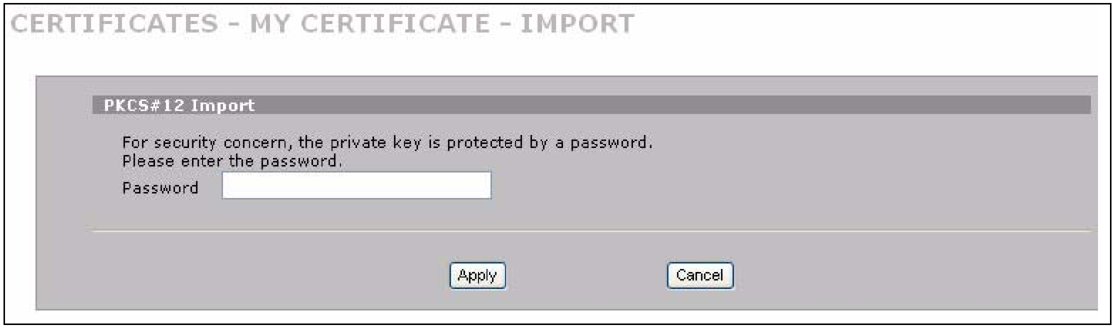
The following table describes the labels in this screen.

**Table 80** SECURITY > CERTIFICATES > My Certificates > Import

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse** to find it. |
| Browse | Click **Browse** to find the certificate file you want to upload. |
| Apply | Click **Apply** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

When you import a binary PKCS#12 format certificate, another screen displays for you to enter the password.

**Figure 202** SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12



For security concern, the private key is protected by a password.
Please enter the password.

The following table describes the labels in this screen.

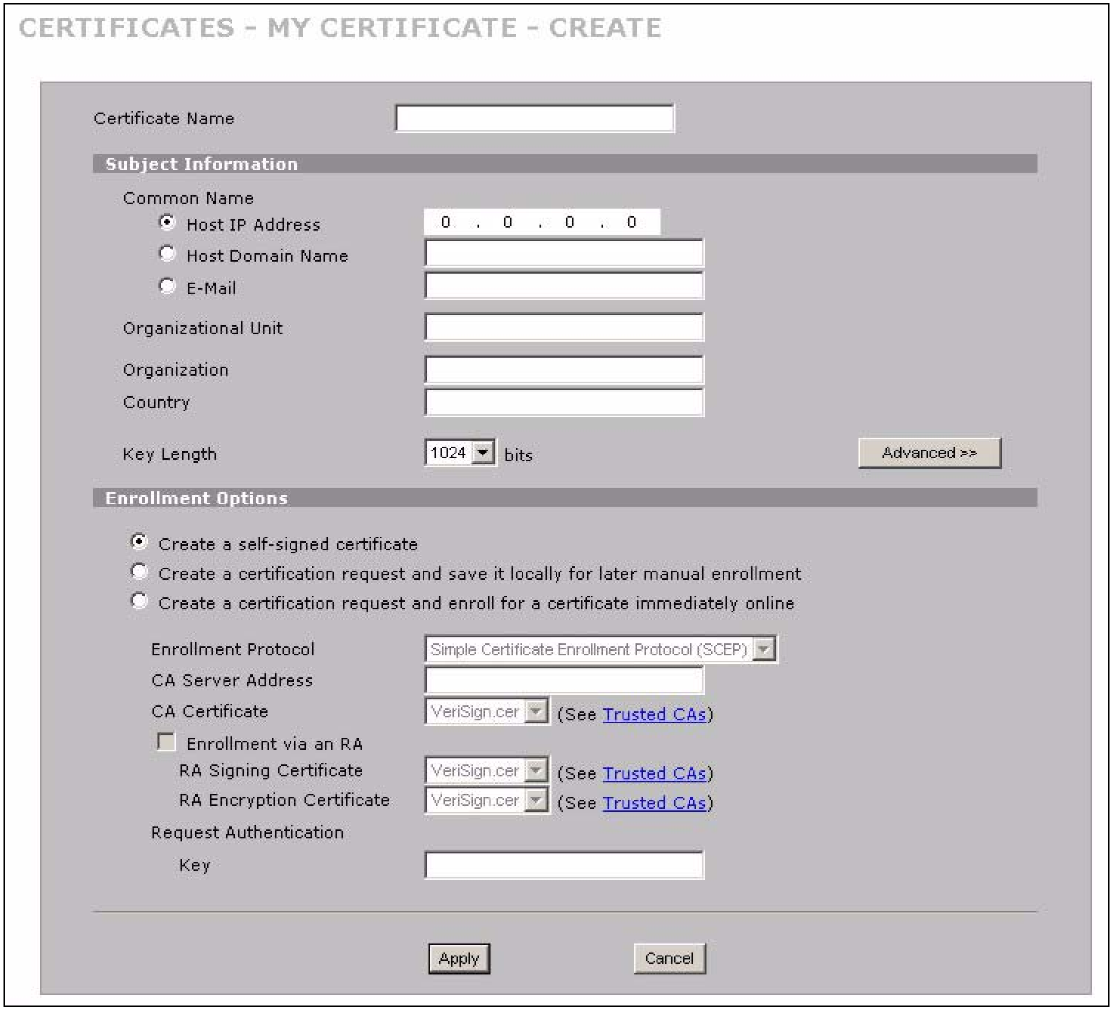
**Table 81** SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12

| LABEL | DESCRIPTION |
|---|---|
| Password | Type the file's password that was created when the PKCS #12 file was exported. |
| Apply | Click **Apply** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

## 15.9 My Certificate Create

Click **SECURITY** > **CERTIFICATES** > **My Certificates > Create** to open the **My Certificate Create** screen. Use this screen to have the ZyWALL create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

**Figure 203** SECURITY > CERTIFICATES > My Certificates > Create (Basic)



CERTIFICATES - MY CERTIFICATE - CREATE

Certificate Name

**Subject Information**

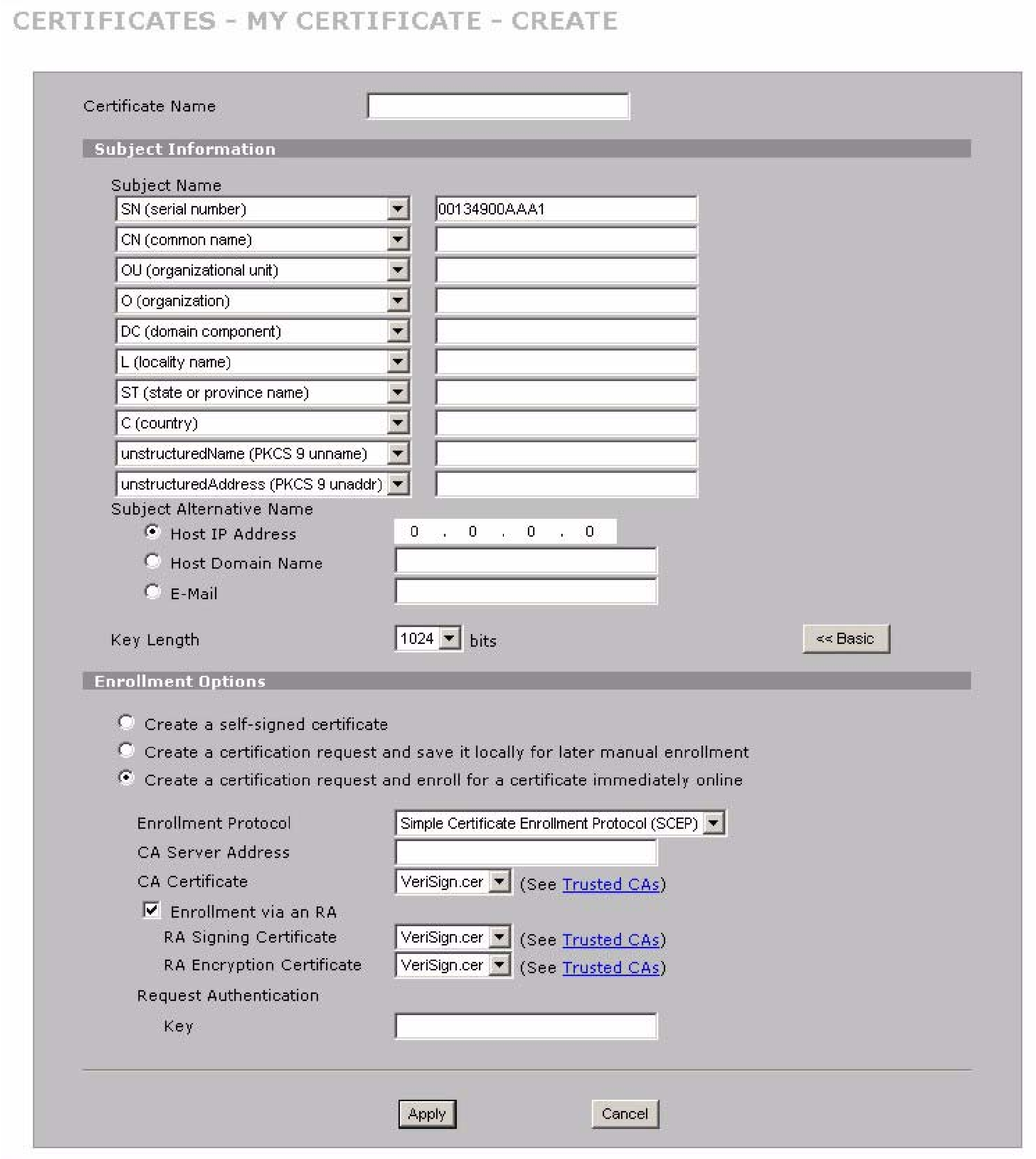
Common Name
● Host IP Address 0 . 0 . 0 . 0
○ Host Domain Name
○ E-Mail
Organizational Unit
Organization
Country
Key Length 1024 bits

**Enrollment Options**

● Create a self-signed certificate
○ Create a certification request and save it locally for later manual enrollment
○ Create a certification request and enroll for a certificate immediately online

Enrollment Protocol Simple Certificate Enrollment Protocol (SCEP)
CA Server Address
CA Certificate VeriSign.cer (See Trusted CAs)
☐ Enrollment via an RA
RA Signing Certificate VeriSign.cer (See Trusted CAs)
RA Encryption Certificate VeriSign.cer (See Trusted CAs)
Request Authentication
Key

**Figure 204** SECURITY > CERTIFICATES > My Certificates > Create (Advanced)


CERTIFICATES - MY CERTIFICATE - CREATE
Certificate Name
Subject Information
Subject Name
CN (common name)
OU (organizational unit)
O (organization)
DC (domain component)
L (locality name)
ST (state or province name)
C (country)
unstructuredName (PKCS 9 unname)
unstructuredAddress (PKCS 9 unaddr)
Subject Alternative Name
Host Domain Name
E-Mail
<< Basic
Enrollment Options
○ Create a self-signed certificate
○ Create a certification request and save it locally for later manual enrollment
CA Server Address
Request Authentication
Key
Apply
Cancel

SN (serial number): 00134900AAA1

● Host IP Address: 0 . 0 . 0 . 0

Key Length: 1024 bits

● Create a certification request and enroll for a certificate immediately online

Enrollment Protocol: Simple Certificate Enrollment Protocol (SCEP)

CA Certificate: VeriSign.cer (See Trusted CAs)

☑ Enrollment via an RA

RA Signing Certificate: VeriSign.cer (See Trusted CAs)

RA Encryption Certificate: VeriSign.cer (See Trusted CAs)

The following table describes the labels in this screen.

**Table 82** SECURITY > CERTIFICATES > My Certificates > Create

| LABEL | DESCRIPTION |
|---|---|
| Certificate Name | Type up to 31 ASCII characters (not including spaces) to identify this certificate. |
| Subject Information | Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, but the **Common Name** is mandatory if you click **<< Basic**. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. |
| The fields below display when you click **<< Basic**. | |

**Table 82** SECURITY > CERTIFICATES > My Certificates > Create (continued)

| LABEL | DESCRIPTION |
|---|---|
| Common Name | Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string. |
| Organizational Unit | Type up to 63 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Organization | Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Country | Type up to 63 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| The fields below display when you click **Advanced >>**. | |
| Subject Name | You must configure at least one of these fields.<br>Select an item from the drop-down list box and enter the corresponding information in the field to the right.<br>**SN (serial number)** - select this and enter the certificate's identification number, such as the ZyWALL's MAC address. You can use up to 63 characters.<br>**CN (common name)** - select this and enter a name to identify the owner of the certificate. You can use up to 63 characters.<br>**OU (organizational unit)** - select this and enter a unit within the organization to identify the owner of the certificate. You can use up to 63 characters.<br>**O (organization)** - select this and enter an organization to identify the owner of the certificate. You can use up to 63 characters.<br>**DC (domain component)** - select this and enter the domain component of a domain to identify the owner of the certificate. For example, if the domain is zyxel.com, the domain component is "zyxel" or "com". You can use up to 63 characters.<br>**L (locality name)** - select this and enter the place where the owner of the certificate resides, such as a city or county. You can use up to 63 characters.<br>**ST (state or province name)** - select this and enter the state or province in which the owner of the certificate resides. You can use up to 63 characters.<br>**C (country)** - select this and enter the name of the country at which the owner of the certificate resides. You can use up to 63 characters.<br>**unstructuredName (PKCS 9 unname)** - select this and enter the name of the owner of the certificate as an unstructured ASCII string. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate.<br>**unstructuredAddress (PKCS 9 unaddr)** - select this and enter the address of the owner of the certificate as an unstructured ASCII string. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate.<br>**MAILTO (PKCS 9 email address)** - select this and enter the email address of the owner of the certificate. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate. |

**Table 82** SECURITY > CERTIFICATES > My Certificates > Create (continued)

| LABEL | DESCRIPTION |
|---|---|
| Subject Alternative Name | Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string. |
| Key Length | Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space. |
| << Basic/Advanced >> | Click **<< Basic** to configure basic subject information. Click **Advanced >>** to configure more subject information for a certificate. |
| Enrollment Options | These radio buttons deal with how and when the certificate is to be generated. |
| Create a self-signed certificate | Select **Create a self-signed certificate** to have the ZyWALL generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates. |
| Create a certification request and save it locally for later manual enrollment | Select **Create a certification request and save it locally for later manual enrollment** to have the ZyWALL generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority.<br>Copy the certification request from the **My Certificate Details** screen (see Section 15.6 on page 300) and then send it to the certification authority. |
| Create a certification request and enroll for a certificate immediately online | Select **Create a certification request and enroll for a certificate immediately online** to have the ZyWALL generate a request for a certificate and apply to a certification authority for a certificate.<br>You must have the certification authority's certificate already imported in the **Trusted CAs** screen.<br>When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them. |
| Enrollment Protocol | Select the certification authority's enrollment protocol from the drop-down list box.<br>**Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.<br>**Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510. |
| CA Server Address | Enter the IP address (or URL) of the certification authority server. |
| CA Certificate | Select the certification authority's certificate from the **CA Certificate** drop-down list box.<br>You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities. |
| Enrollment via an RA | If you select **Create a certification request and enroll for a certificate immediately online**, you can select this option to apply for a certificate through a RA (Registration Authority). The RA is an intermediary authorized by a CA to verify each subscriber's identity and forward the requests to the CA. After the CA signs and issues the certificates, the RA distributes the certificates to the subscribers. |

**Table 82** SECURITY > CERTIFICATES > My Certificates > Create (continued)

| LABEL | DESCRIPTION |
|---|---|
| RA Signing Certificate | If you select **Enrollment via an RA**, select the CA's RA signing certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen.<br>Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities. |
| RA Encryption Certificate | If you select **Enrollment via an RA**, select the CA's RA encryption certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen.<br>Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities. |
| Request Authentication | When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SCEP enrollment protocol. |
| Reference Number | Enter the reference number that the certification authority gave you. You can use up to 31 ASCII printable characters. Spaces are allowed. |
| Key | Type the key that the certification authority gave you. You can use up to 31 ASCII printable characters. Spaces are allowed. |
| Apply | Click **Apply** to begin certificate or certification request generation. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyWALL is generating the self-signed certificate or certification request.

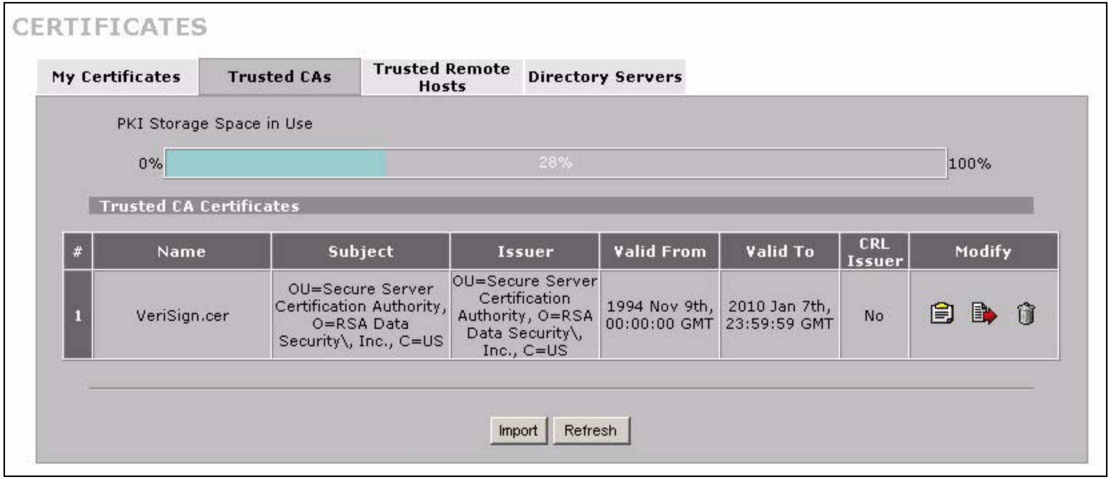
After the ZyWALL successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the ZyWALL enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyWALL to enroll a certificate online.

## 15.10 Trusted CAs

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyWALL to accept as trusted. The ZyWALL accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

**Figure 205** SECURITY > CERTIFICATES > Trusted CAs



| # | Name | Subject | Issuer | Valid From | Valid To | CRL Issuer | Modify |
|---|---|---|---|---|---|---|---|
| 1 | VeriSign.cer | OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US | OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US | 1994 Nov 9th, 00:00:00 GMT | 2010 Jan 7th, 23:59:59 GMT | No | |

The following table describes the labels in this screen.

**Table 83** SECURITY > CERTIFICATES > Trusted CAs

| LABEL | DESCRIPTION |
|---|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| # | This field displays the certificate index number. The certificates are listed in alphabetical order. |
| Name | This field displays the name used to identify this certificate. |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field. |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| CRL Issuer | This field displays **Yes** if the certification authority issues CRL (Certificate Revocation Lists) for the certificates that it has issued and you have selected the **Check incoming certificates issued by this CA against a CRL** check box in the certificate's details screen to have the ZyWALL check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays **No**. |
| Modify | Click the details icon to open a screen with an in-depth list of information about the certificate.<br>Use the export icon to save the certificate to a computer. Click the icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.<br>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action. |

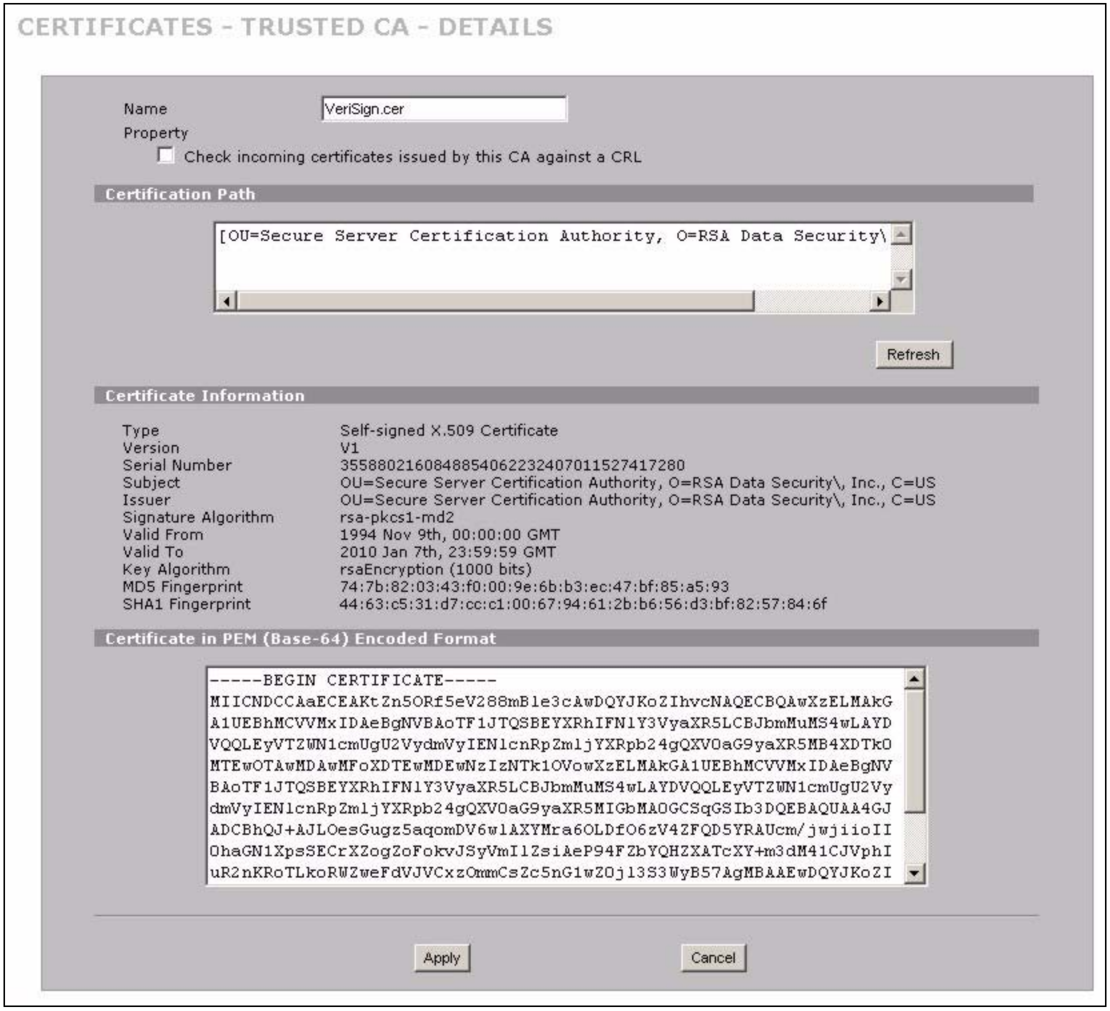
**Table 83** SECURITY > CERTIFICATES > Trusted CAs (continued)

| LABEL | DESCRIPTION |
|---|---|
| Import | Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyWALL. |
| Refresh | Click this button to display the current validity status of the certificates. |

## 15.11 Trusted CA Details

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyWALL to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

**Figure 206** SECURITY > CERTIFICATES > Trusted CAs > Details


CERTIFICATES - TRUSTED CA - DETAILS
Certification Path
Refresh
Certificate Information
Certificate in PEM (Base-64) Encoded Format
Apply
Cancel

Name: VeriSign.cer

Property

☐ Check incoming certificates issued by this CA against a CRL

[OU=Secure Server Certification Authority, O=RSA Data Security\

| | |
|---|---|
| Type | Self-signed X.509 Certificate |
| Version | V1 |
| Serial Number | 3558802160848854062232407011527417280 |
| Subject | OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US |
| Issuer | OU=Secure Server Certification Authority, O=RSA Data Security\, Inc., C=US |
| Signature Algorithm | rsa-pkcs1-md2 |
| Valid From | 1994 Nov 9th, 00:00:00 GMT |
| Valid To | 2010 Jan 7th, 23:59:59 GMT |
| Key Algorithm | rsaEncryption (1000 bits) |
| MD5 Fingerprint | 74:7b:82:03:43:f0:00:9e:6b:b3:ec:47:bf:85:a5:93 |
| SHA1 Fingerprint | 44:63:c5:31:d7:cc:c1:00:67:94:61:2b:b6:56:d3:bf:82:57:84:6f |

```
-----BEGIN CERTIFICATE-----
MIICNDCCAaECEAKtZn5ORf5eV288mBle3cAwDQYJKoZIhvcNAQECBQAwXzELMAkG
A1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRhIFN1Y3VyaXR5LCBJbmMuMS4wLAYD
VQQLEyVTZWN1cmUgU2VydmVyIEN1cnRpZm1jYXRpb24gQXV0aG9yaXR5MB4XDTk0
MTEwOTAwMDAwMFoXDTEwMDEwNzIzNTk1OVowXzELMAkGA1UEBhMCVVMxIDAeBgNV
BAoTF1JTQSBEYXRhIFN1Y3VyaXR5LCBJbmMuMS4wLAYDVQQLEyVTZWN1cmUgU2Vy
dmVyIEN1cnRpZm1jYXRpb24gQXV0aG9yaXR5MIGbMA0GCSqGSIb3DQEBAQUAA4GJ
ADCBhQJ+AJLOesGugz5aqomDV6wlAXYMra6OLDfO6zV4ZFQD5YRAUcm/jwjiioII
OhaGN1XpsSECrXZogZoFokvJSyVmIlZsiAeP94FZbYQHZXATcXY+m3dM41CJVphI
uR2nKRoTLkoRWZweFdVJVCxzOmmCsZc5nG1wZOjl3S3WyB57AgMBAAEwDQYJKoZI
```

The following table describes the labels in this screen.

**Table 84** SECURITY > CERTIFICATES > Trusted CAs > Details

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces). |
| Property<br>Check incoming certificates issued by this CA against a CRL | Select this check box to have the ZyWALL check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).<br>Clear this check box to have the ZyWALL not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). |
| Certification Path | Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyWALL does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked. |
| Refresh | Click **Refresh** to display the certification path. |
| Certificate Information | These read-only fields display detailed information about the certificate. |
| Type | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates. |
| Version | This field displays the X.509 version number. |
| Serial Number | This field displays the certificate's identification number given by the certification authority. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br>With self-signed certificates, this is the same information as in the **Subject Name** field. |
| Signature Algorithm | This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example). |
| Subject Alternative Name | This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL). |

**Table 84** SECURITY > CERTIFICATES > Trusted CAs > Details (continued)

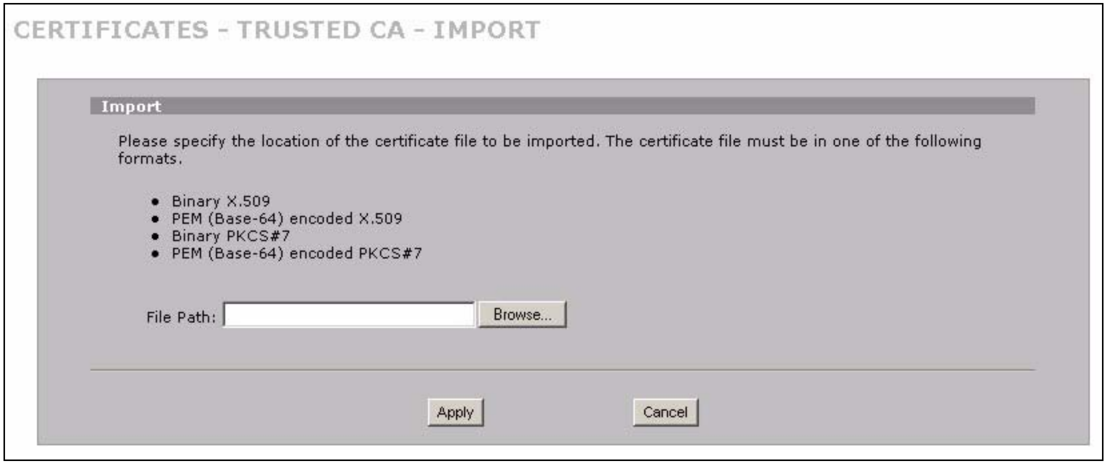
| LABEL | DESCRIPTION |
|---|---|
| Key Usage | This field displays for what functions the certificate’s key can be used. For example, “DigitalSignature” means that the key can be used to sign certificates and “KeyEncipherment” means that the key can be used to encrypt text. |
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority’s certificate and “Path Length Constraint=1” means that there can only be one certification authority in the certificate’s path. |
| CRL Distribution Points | This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers. |
| MD5 Fingerprint | This is the certificate’s message digest that the ZyWALL calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate. |
| SHA1 Fingerprint | This is the certificate’s message digest that the ZyWALL calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.<br>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. You can only change the name and/or set whether or not you want the ZyWALL to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority. |
| Cancel | Click **Cancel** to quit and return to the **Trusted CAs** screen. |

## 15.12 Trusted CA Import

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority’s certificate from a computer to the ZyWALL. The ZyWALL trusts any valid certificate signed by any of the imported trusted CA certificates.

You must remove any spaces from the certificate’s filename before you can import the certificate.

**Figure 207** SECURITY > CERTIFICATES > Trusted CAs > Import



CERTIFICATES - TRUSTED CA - IMPORT

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path:

The following table describes the labels in this screen.

**Table 85** SECURITY > CERTIFICATES > Trusted CAs Import

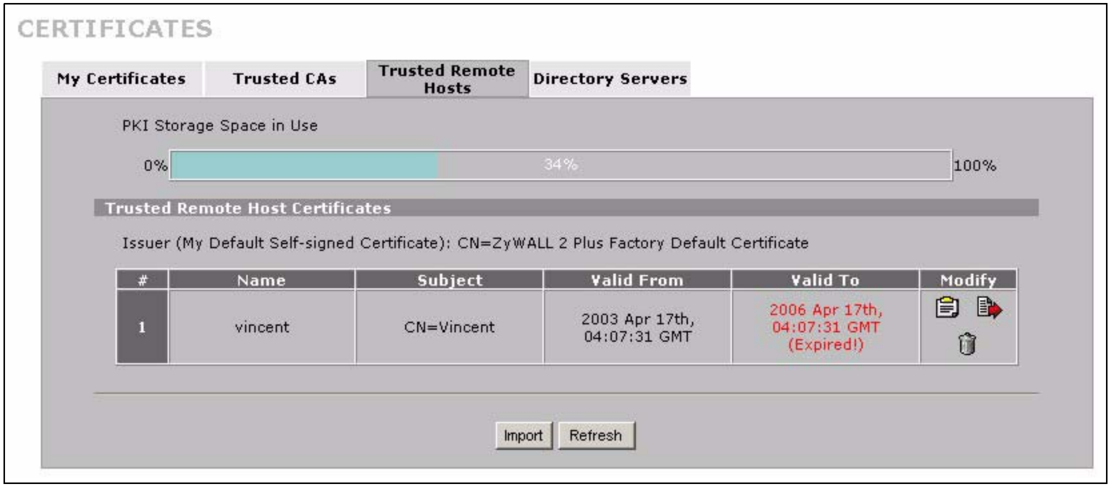
| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse** to find it. |
| Browse | Click **Browse** to find the certificate file you want to upload. |
| Apply | Click **Apply** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the **Trusted CAs** screen. |

## 15.13 Trusted Remote Hosts

Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyWALL automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

**Figure 208** SECURITY > CERTIFICATES > Trusted Remote Hosts



CERTIFICATES

PKI Storage Space in Use

Trusted Remote Host Certificates

Issuer (My Default Self-signed Certificate): CN=ZyWALL 2 Plus Factory Default Certificate

| # | Name | Subject | Valid From | Valid To | Modify |
|---|---|---|---|---|---|
| 1 | vincent | CN=Vincent | 2003 Apr 17th, 04:07:31 GMT | 2006 Apr 17th, 04:07:31 GMT (Expired!) | |

The following table describes the labels in this screen.

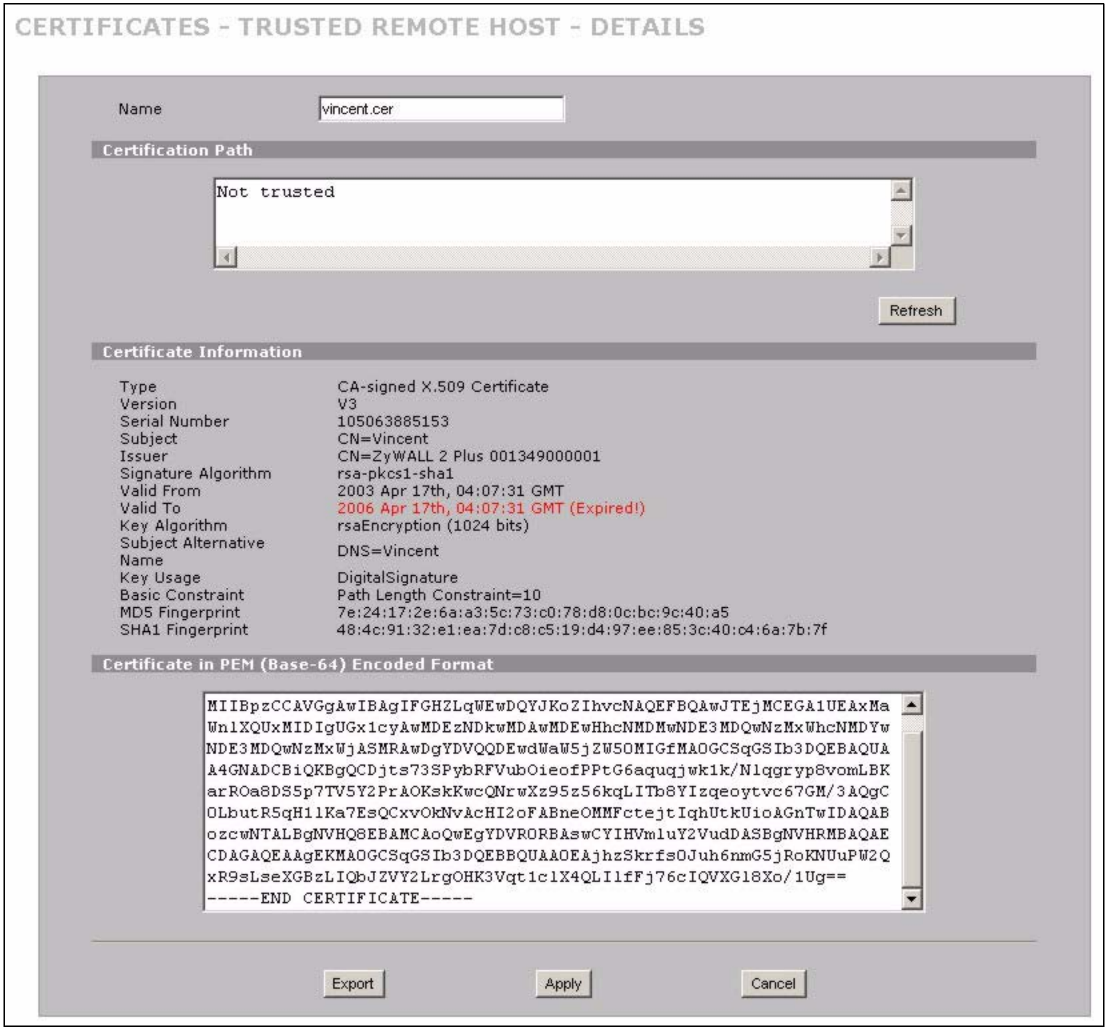
**Table 86** SECURITY > CERTIFICATES > Trusted Remote Hosts

| LABEL | DESCRIPTION |
|---|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| Issuer (My Default Self-signed Certificate) | This field displays identifying information about the default self-signed certificate on the ZyWALL that the ZyWALL uses to sign the trusted remote host certificates. |
| # | This field displays the certificate index number. The certificates are listed in alphabetical order. |
| Name | This field displays the name used to identify this certificate. |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Modify | Click the details icon to open a screen with an in-depth list of information about the certificate.<br>Use the export icon to save the certificate to a computer. Click the icon and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.<br>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action. |
| Import | Click **Import** to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the ZyWALL. |
| Refresh | Click this button to display the current validity status of the certificates. |

## 15.14 Trusted Remote Host Certificate Details

Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. You can use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

**Figure 209** SECURITY > CERTIFICATES > Trusted Remote Hosts > Details


CERTIFICATES - TRUSTED REMOTE HOST - DETAILS
Certification Path
Refresh
Certificate Information
Certificate in PEM (Base-64) Encoded Format
Export
Apply
Cancel

Name: vincent.cer

Not trusted

| | |
|---|---|
| Type | CA-signed X.509 Certificate |
| Version | V3 |
| Serial Number | 105063885153 |
| Subject | CN=Vincent |
| Issuer | CN=ZyWALL 2 Plus 001349000001 |
| Signature Algorithm | rsa-pkcs1-sha1 |
| Valid From | 2003 Apr 17th, 04:07:31 GMT |
| Valid To | 2006 Apr 17th, 04:07:31 GMT (Expired!) |
| Key Algorithm | rsaEncryption (1024 bits) |
| Subject Alternative Name | DNS=Vincent |
| Key Usage | DigitalSignature |
| Basic Constraint | Path Length Constraint=10 |
| MD5 Fingerprint | 7e:24:17:2e:6a:a3:5c:73:c0:78:d8:0c:bc:9c:40:a5 |
| SHA1 Fingerprint | 48:4c:91:32:e1:ea:7d:c8:c5:19:d4:97:ee:85:3c:40:c4:6a:7b:7f |

```
MIIBpzCCAVGgAwIBAgIFGHZLqWEwDQYJKoZIhvcNAQEFBQAwJTEjMCEGA1UEAxMa
WnlXQUxMIDIgUGx1cyAwMDEzNDkwMDAwMDEwHhcNMDMwNDE3MDQwNzMxWhcNMDYw
NDE3MDQwNzMxWjASMRAwDgYDVQQDEwdWaW5jZW50MIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCDjts73SPybRFVubOieofPPtG6aquqjwk1k/Nlqgryp8vomLBK
arROa8DS5p7TV5Y2PrAOKskKwcQNrwXz95z56kqLITb8YIzqeoytvc67GM/3AQgC
OLbutR5qH1lKa7EsQCxvOkNvAcHI2oFABneOMMFctejtIqhUtkUioAGnTwIDAQAB
ozcwNTALBgNVHQ8EBAMCAoQwEgYDVR0RBAswCYIHVmluY2VudDASBgNVHRMBAQAE
CDAGAQEAAgEKMA0GCSqGSIb3DQEBBQUAA0EAjhzSkrfs0Juh6nmG5jRoKNUuPW2Q
xR9sLseXGBzLIQbJZVY2LrgOHK3Vqt1clX4QLIlfFj76cIQVXGl8Xo/1Ug==
-----END CERTIFICATE-----
```

The following table describes the labels in this screen.

**Table 87** SECURITY > CERTIFICATES > Trusted Remote Hosts > Details

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces). |
| Certification Path | Click the **Refresh** button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the ZyWALL uses to sign remote host certificates. |
| Refresh | Click **Refresh** to display the certification path. |
| Certificate Information | These read-only fields display detailed information about the certificate. |
| Type | This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The ZyWALL is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates. |

**Table 87** SECURITY > CERTIFICATES > Trusted Remote Hosts > Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| Version | This field displays the X.509 version number. |
| Serial Number | This field displays the certificate's identification number given by the device that created the certificate. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Issuer | This field displays identifying information about the default self-signed certificate on the ZyWALL that the ZyWALL uses to sign the trusted remote host certificates. |
| Signature Algorithm | This field displays the type of algorithm that the ZyWALL used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example). |
| Subject Alternative Name | This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL). |
| Key Usage | This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text. |
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. |
| MD5 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. The ZyWALL uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section 15.3 on page 296 for how to verify a remote host's certificate before you import it into the ZyWALL. |
| SHA1 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. The ZyWALL uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section 15.3 on page 296 for how to verify a remote host's certificate before you import it into the ZyWALL. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.<br>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |

**Table 87** SECURITY > CERTIFICATES > Trusted Remote Hosts > Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. You can only change the name of the certificate. |
| Cancel | Click **Cancel** to quit configuring this screen and return to the **Trusted Remote Hosts** screen. |

## 15.15 Trusted Remote Hosts Import

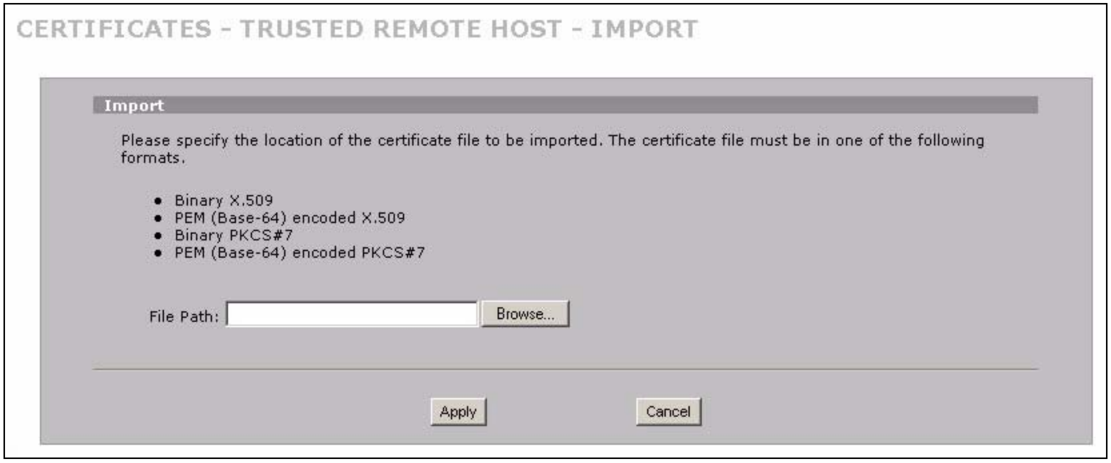
Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen.

You may have peers with certificates that you want to trust, but the certificates were not signed by one of the certification authorities on the **Trusted CAs** screen. Follow the instructions in this screen to save a peer's certificates from a computer to the ZyWALL.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyWALL automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its filename before you can import it.

**Figure 210** SECURITY > CERTIFICATES > Trusted Remote Hosts > Import



Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

The following table describes the labels in this screen.

**Table 88** SECURITY > CERTIFICATES > Trusted Remote Hosts > Import

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse** to find it. |
| Browse | Click **Browse** to find the certificate file you want to upload. |

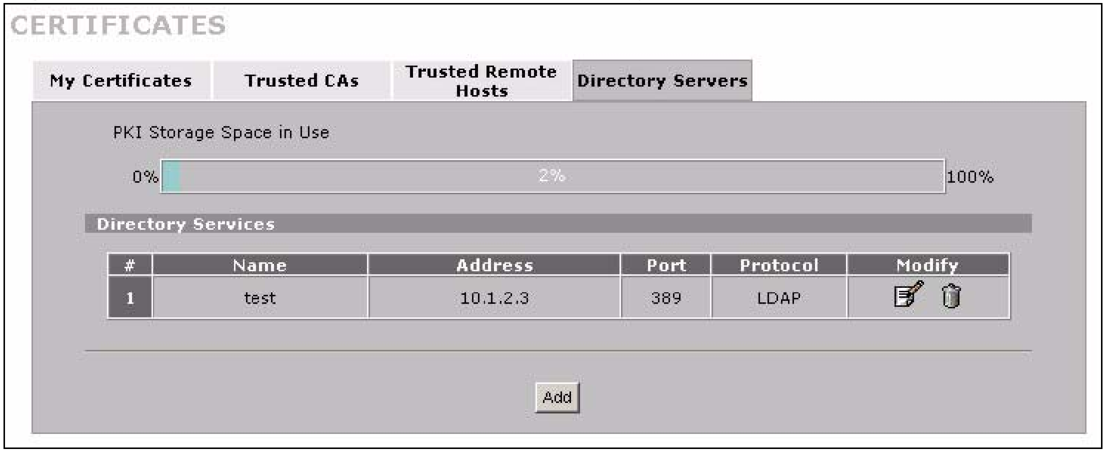
**Table 88** SECURITY > CERTIFICATES > Trusted Remote Hosts > Import

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the **Trusted Remote Hosts** screen. |

## 15.16 Directory Servers

Click **SECURITY** > **CERTIFICATES** > **Directory Servers** to open the **Directory Servers** screen. This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the ZyWALL. If you decide to have the ZyWALL check incoming certificates against the issuing certification authority's list of revoked certificates, the ZyWALL first checks the server(s) listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the ZyWALL checks the servers listed here.

**Figure 211** SECURITY > CERTIFICATES > Directory Servers



| # | Name | Address | Port | Protocol | Modify |
|---|---|---|---|---|---|
| 1 | test | 10.1.2.3 | 389 | LDAP | |

The following table describes the labels in this screen.

**Table 89** SECURITY > CERTIFICATES > Directory Servers

| LABEL | DESCRIPTION |
|---|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| # | The index number of the directory server. The servers are listed in alphabetical order. |
| Name | This field displays the name used to identify this directory server. |
| Address | This field displays the IP address or domain name of the directory server. |
| Port | This field displays the port number that the directory server uses. |
| Protocol | This field displays the protocol that the directory server uses. |

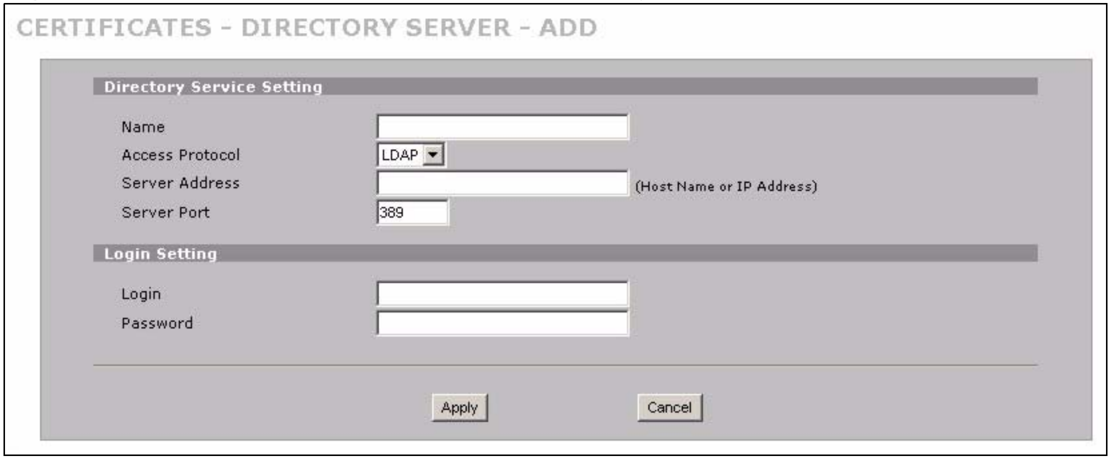
**Table 89** SECURITY > CERTIFICATES > Directory Servers

| LABEL | DESCRIPTION |
|---|---|
| Modify | Click the details icon to open a screen where you can change the information about the directory server.<br>Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action. |
| Add | Click **Add** to open a screen where you can configure information about a directory server so that the ZyWALL can access it. |

## 15.17 Directory Server Add or Edit

Click **SECURITY** > **CERTIFICATES** > **Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the **Directory Server Add** screen. Use this screen to configure information about a directory server that the ZyWALL can access.

**Figure 212** SECURITY > CERTIFICATES > Directory Server > Add



CERTIFICATES - DIRECTORY SERVER - ADD

Directory Service Setting

Name

Access Protocol: LDAP

Server Address (Host Name or IP Address)

Server Port: 389

Login Setting

Login

Password

The following table describes the labels in this screen.

**Table 90** SECURITY > CERTIFICATES > Directory Server > Add

| LABEL | DESCRIPTION |
|---|---|
| Directory Service Setting | |
| Name | Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server. |
| Access Protocol | Use the drop-down list box to select the access protocol used by the directory server.<br>**LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.[A] |
| Server Address | Type the IP address (in dotted decimal notation) or the domain name of the directory server. |

**Table 90** SECURITY > CERTIFICATES > Directory Server > Add

| LABEL | DESCRIPTION |
|---|---|
| Server Port | This field displays the default server port number of the protocol that you select in the **Access Protocol** field.<br>You may change the server port number if needed, however you must use the same server port number that the directory server uses.<br>389 is the default server port number for LDAP. |
| Login Setting | |
| Login | The ZyWALL may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority). |
| Password | Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to quit configuring this screen and return to the **Directory Servers** screen. |

A. At the time of writing, LDAP is the only choice of directory server access protocol.

# 16

# Authentication Server

This chapter discusses how to configure the ZyWALL's authentication server feature.

## 16.1 Authentication Server Overview

A ZyWALL set to be a VPN extended authentication server can use either the local user database internal to the ZyWALL or an external RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) server for an unlimited number of users. The ZyWALL uses the same local user database for VPN extended authentication.

### 16.1.1 Local User Database

By storing user profiles locally on the ZyWALL, your ZyWALL is able to authenticate users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

### 16.1.2 RADIUS

The ZyWALL can use a RADIUS server to authenticate an unlimited number of users. RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
  Determines the identity of the users.
- Authorization
  Determines the network services available to authenticated users once they are connected to the network.
- Accounting
  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which the ZyWALL acts as a message relay between the client and the network RADIUS server.

### 16.1.3 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the ZyWALL and the RADIUS server for user authentication:

- Access-Request

Sent by an access point requesting authentication.

- Access-Reject
  Sent by a RADIUS server rejecting access.
- Access-Accept
  Sent by a RADIUS server allowing access.
- Access-Challenge
  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the ZyWALL and the RADIUS server for user accounting:

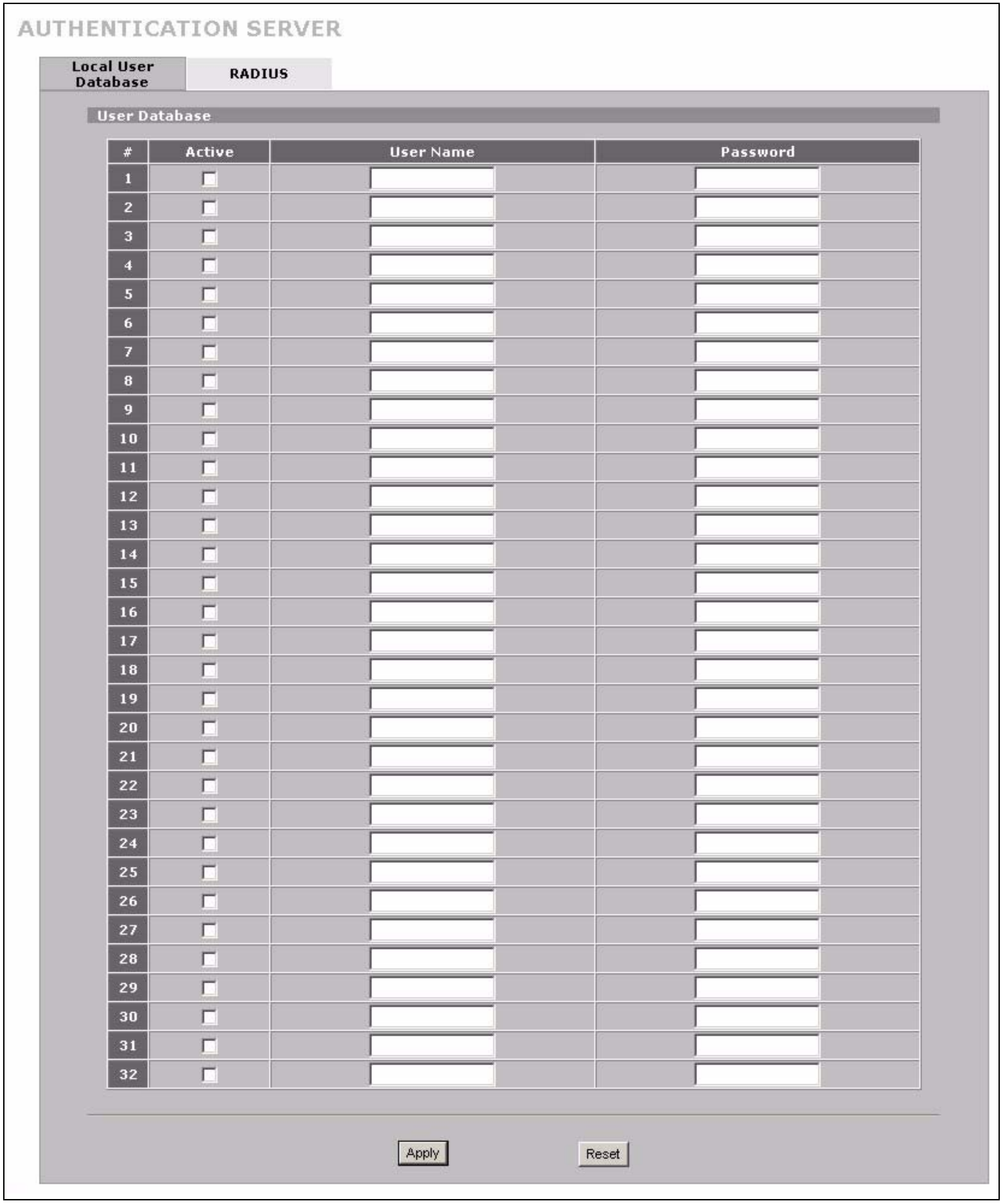
- Accounting-Request
  Sent by the access point requesting accounting.
- Accounting-Response
  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the ZyWALL and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

## 16.2 Local User Database

Click **SECURITY** > **AUTH SERVER** to open the **Local User Database** screen. The local user database is a list of user profiles stored on the ZyWALL. The ZyWALL can use this list of user profiles to authenticate users. Use this screen to change your ZyWALL's list of user profiles.

**Figure 213** SECURITY > AUTH SERVER > Local User Database


AUTHENTICATION SERVER
Local User Database
RADIUS
User Database
#
Active
User Name
Password
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
Apply
Reset

The following table describes the labels in this screen.

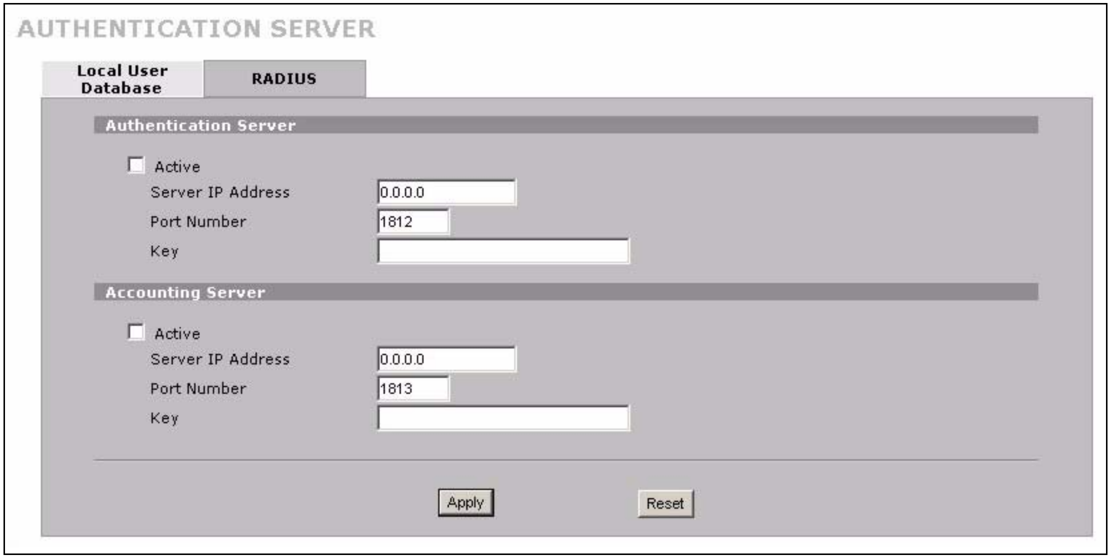
**Table 91** SECURITY > AUTH SERVER > Local User Database

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to enable the user profile. |
| User Name | Enter the user name of the user profile. |
| Password | Enter a password up to 31 characters long for this user profile. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 16.3 RADIUS

Click **SECURITY** > **AUTH SERVER** > **RADIUS** to open the **RADIUS** screen. Configure this screen to use an external RADIUS server to authenticate users.

**Figure 214** SECURITY > AUTH SERVER > RADIUS



☐ Active
Server IP Address 0.0.0.0
Port Number 1812
Key

☐ Active
Server IP Address 0.0.0.0
Port Number 1813
Key

The following table describes the labels in this screen.

**Table 92** SECURITY > AUTH SERVER > RADIUS

| LABEL | DESCRIPTION |
|---|---|
| Authentication Server | |
| Active | Select the check box to enable user authentication through an external authentication server.<br>Clear the check box to enable user authentication using the local user profile on the ZyWALL. |
| Server IP Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port Number | The default port of the RADIUS server for authentication is **1812**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Key | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL.<br>The key is not sent over the network. This key must be the same on the external authentication server and ZyWALL. |
| Accounting Server | |
| Active | Select the check box to enable user accounting through an external authentication server. |
| Server IP Address | Enter the IP address of the external accounting server in dotted decimal notation. |
| Port Number | The default port of the RADIUS server for accounting is **1813**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |

**Table 92** SECURITY > AUTH SERVER > RADIUS

| LABEL | DESCRIPTION |
|---|---|
| Key | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyWALL.<br>The key is not sent over the network. This key must be the same on the external accounting server and ZyWALL. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# PART IV

# Advanced

Network Address Translation (NAT) (331)
Static Route (347)
Bandwidth Management (351)
DNS (365)
Remote Management (377)
UPnP (399)
ALG Screen (411)

17

# Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

## 17.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

### 17.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyWALL. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 93** NAT Definitions

| TERM | DESCRIPTION |
|---|---|
| Inside | This refers to the host on the LAN. |
| Outside | This refers to the host on the WAN. |
| Local | This refers to the packet address (source or destination) as the packet travels on the LAN. |
| Global | This refers to the packet address (source or destination) as the packet travels on the WAN. |

NAT never changes the IP address (either local or global) of an outside host.

### 17.1.2 What NAT Does

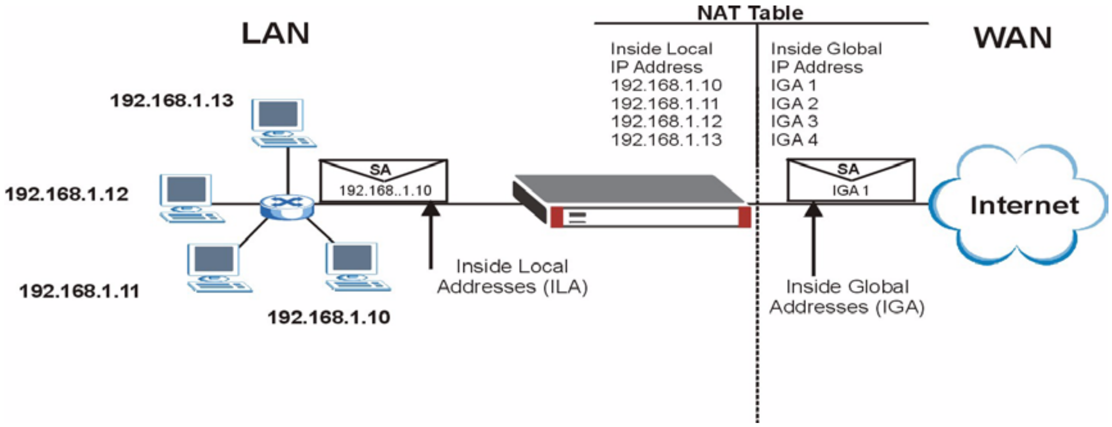
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyWALL filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

### 17.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyWALL keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

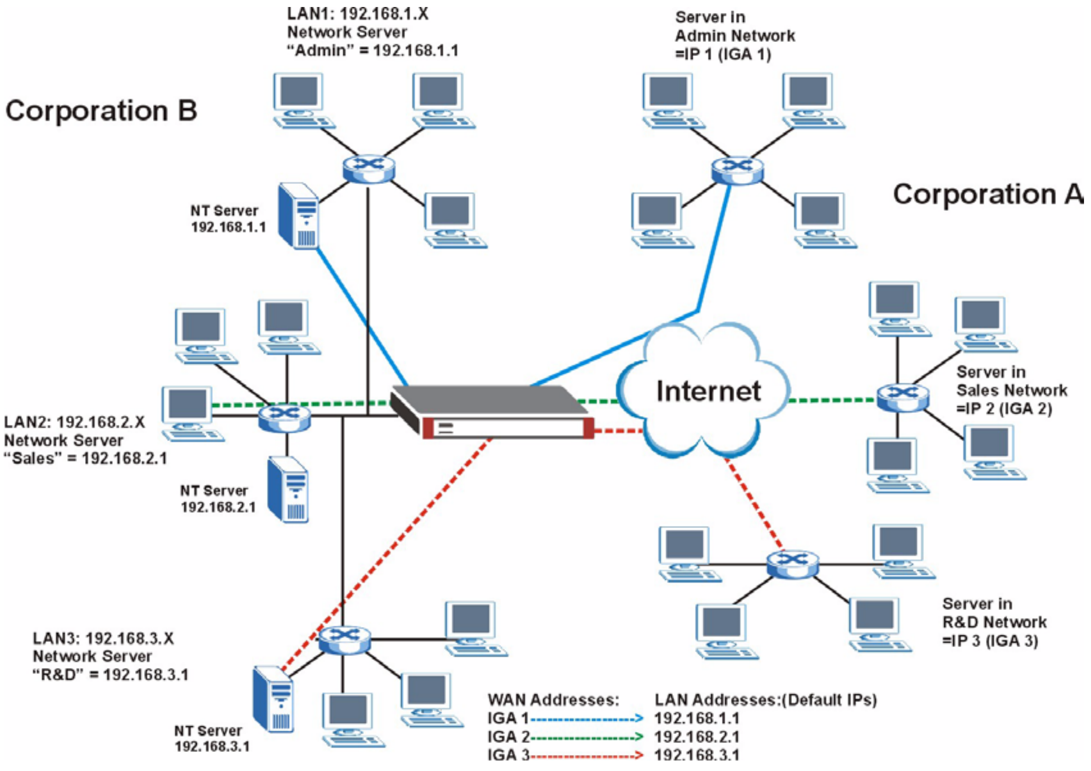
**Figure 215** How NAT Works


LAN
NAT Table
Inside Local
IP Address
192.168.1.10
192.168.1.11
192.168.1.12
192.168.1.13
Inside Global
IP Address
IGA 1
IGA 2
IGA 3
IGA 4
WAN
192.168.1.13
192.168.1.12
192.168.1.11
192.168.1.10
SA
192.168..1.10
Inside Local
Addresses (ILA)
SA
IGA 1
Internet
Inside Global
Addresses (IGA)

## 17.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the ZyWALL can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

**Figure 216** NAT Application With IP Alias


LAN1: 192.168.1.X
Network Server
"Admin" = 192.168.1.1
Server in
Admin Network
=IP 1 (IGA 1)
Corporation B
Corporation A
NT Server
192.168.1.1
Internet
Server in
Sales Network
=IP 2 (IGA 2)
LAN2: 192.168.2.X
Network Server
"Sales" = 192.168.2.1
NT Server
192.168.2.1
Server in
R&D Network
=IP 3 (IGA 3)
LAN3: 192.168.3.X
Network Server
"R&D" = 192.168.3.1
NT Server
192.168.3.1
WAN Addresses:
LAN Addresses:(Default IPs)
IGA 1-------------------> 192.168.1.1
IGA 2-------------------> 192.168.2.1
IGA 3-------------------> 192.168.3.1

### 17.1.5 Port Restricted Cone NAT

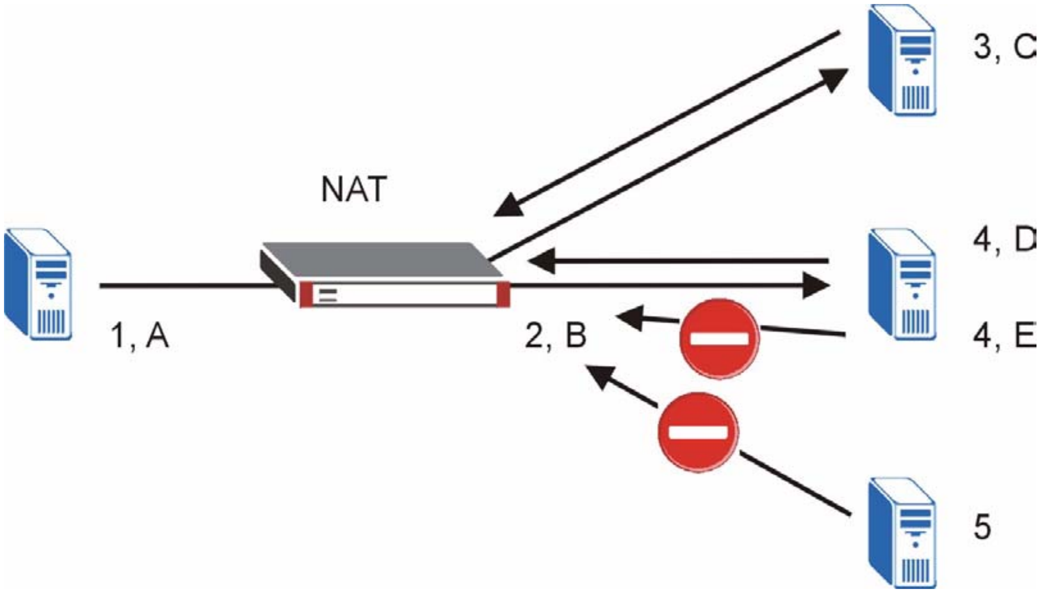
ZyWALL ZyNOS version 4.00 and later uses port restricted cone NAT. Port restricted cone NAT maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the ZyWALL maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. A host on the external network (IP address **3** and Port **C** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address and port.

A server with IP address **1** and port **A** sends packets to IP address **3**, port **C** and IP address **4**, port **D**. The ZyWALL changes the server's IP address to **2** and port to **B**.

Since **1**, **A** has already sent packets to **3**, **C** and **4**, **D,** they can send packets back to **2**, **B** and the ZyWALL will perform NAT on them and send them to the server at IP address **1**, port **A**.

Packets have not been sent from **1**, **A** to **4**, **E** or **5**, so they cannot send packets to **1**, **A**.

**Figure 217** Port Restricted Cone NAT Example



### 17.1.6 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyWALL maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyWALL maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the **SUA** option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyWALL maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the ZyWALL maps each local IP address to a unique global IP address.

- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

Port numbers do not change for One-to-One and Many-One-to-One NAT mapping types.

The following table summarizes the NAT mapping types.

**Table 94** NAT Mapping Types

| TYPE | IP MAPPING | SMT ABBREVIATION |
|---|---|---|
| One-to-One | ILA1 ←→ IGA1 | 1-1 |
| Many-to-One (SUA/PAT) | ILA1 ←→ IGA1<br>ILA2 ←→ IGA1<br>… | M-1 |
| Many-to-Many Overload | ILA ←→ IGA1<br>ILA2 ←→ IGA2<br>ILA3 ←→ IGA1<br>ILA4 ←→ IGA2<br>… | M-M Ov |
| Many-One-to-One | ILA1 ←→ IGA1<br>ILA2 ←→ IGA2<br>ILA3 ←→ IGA3<br>… | M-1-1 |
| Server | Server 1 IP ←→ IGA1<br>Server 2 IP ←→ IGA1<br>Server 3 IP ←→ IGA1 | Server |

## 17.2 Using NAT

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyWALL.

### 17.2.1 SUA (Single User Account) Versus NAT

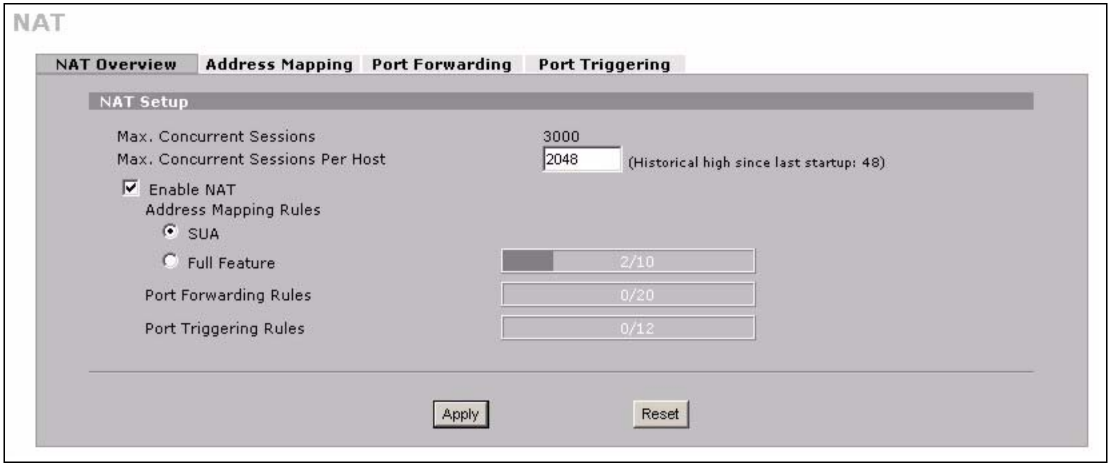
SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA** or **Full Feature** in **NAT Overview**.

Selecting **SUA** means (latent) multiple WAN-to-LAN and WAN-to-DMZ address translation. That means that computers on your DMZ with public IP addresses will still have to undergo NAT mapping if you're using **SUA** NAT mapping. If this is not your intention, then select **Full Feature** NAT and don't configure NAT mapping rules to those computers with public IP addresses on the DMZ.

## 17.3 NAT Overview Screen

Click **ADVANCED** > **NAT** to open the **NAT Overview** screen.

**Figure 218** ADVANCED > NAT > NAT Overview



Max. Concurrent Sessions 3000
Max. Concurrent Sessions Per Host 2048 (Historical high since last startup: 48)
☑ Enable NAT
Address Mapping Rules
● SUA
○ Full Feature 2/10
Port Forwarding Rules 0/20
Port Triggering Rules 0/12

The following table describes the labels in this screen.

**Table 95** ADVANCED > NAT > NAT Overview

| LABEL | DESCRIPTION |
|---|---|
| NAT Setup | |
| Max. Concurrent Sessions | This read-only field displays the highest number of NAT sessions that the ZyWALL will permit at one time. |
| Max. Concurrent Sessions Per Host | Use this field to set the highest number of NAT sessions that the ZyWALL will permit a host to have at one time. |
| Enable NAT | Select this check box to turn on the NAT feature for the WAN port. Clear this check box to turn off the NAT feature for the WAN port. |
| Address Mapping Rules | Select **SUA** if you have just one public WAN IP address for your ZyWALL. This lets the ZyWALL use its permanent, pre-defined NAT address mapping rules.<br>Select **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL. This lets the ZyWALL use the address mapping rules that you configure. This is the equivalent of what used to be called full feature NAT or multi-NAT.<br>The bar displays how many of the ZyWALL's possible address mapping rules are configured. The first number shows how many address mapping rules are configured on the ZyWALL. The second number shows the maximum number of address mapping rules that can be configured on the ZyWALL. |

**Table 95** ADVANCED > NAT > NAT Overview (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port Forwarding Rules | The bar displays how many of the ZyWALL's possible port forwarding rules are configured. The first number shows how many port forwarding rules are configured on the ZyWALL. The second number shows the maximum number of port forwarding rules that can be configured on the ZyWALL. |
| Port Triggering Rules | The bar displays how many of the ZyWALL's possible trigger port rules are configured. The first number shows how many trigger port rules are configured on the ZyWALL. The second number shows the maximum number of trigger port rules that can be configured on the ZyWALL. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 17.4 NAT Address Mapping

Click **ADVANCED** > **NAT** > **Address Mapping** to open the following screen.

### 17.4.1 What NAT Does

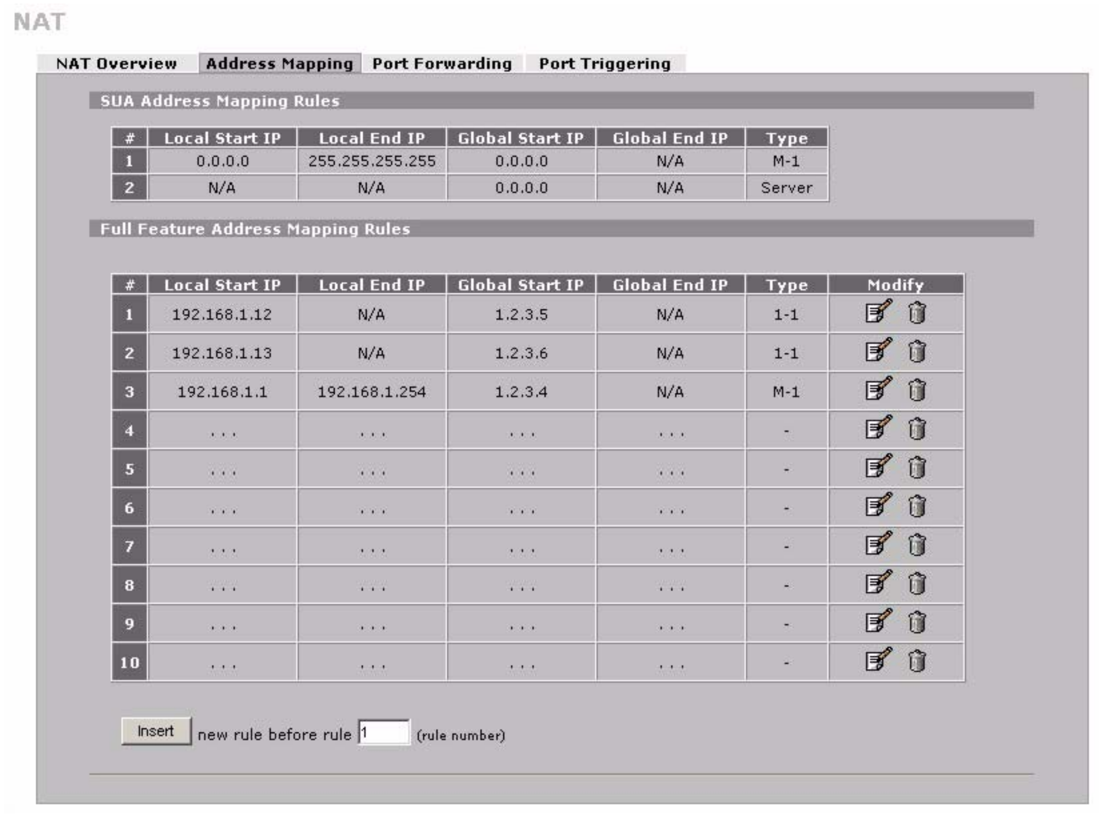
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

See Section 17.1 on page 331 for more on NAT.

Use this screen to change your ZyWALL’s address mapping settings.

Ordering your rules is important because the ZyWALL applies the rules in the order that you specify. When a rule matches the current packet, the ZyWALL takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

**Figure 219** ADVANCED > NAT > Address Mapping



SUA Address Mapping Rules

| # | Local Start IP | Local End IP | Global Start IP | Global End IP | Type |
|---|---|---|---|---|---|
| 1 | 0.0.0.0 | 255.255.255.255 | 0.0.0.0 | N/A | M-1 |
| 2 | N/A | N/A | 0.0.0.0 | N/A | Server |

Full Feature Address Mapping Rules

| # | Local Start IP | Local End IP | Global Start IP | Global End IP | Type | Modify |
|---|---|---|---|---|---|---|
| 1 | 192.168.1.12 | N/A | 1.2.3.5 | N/A | 1-1 | ✎ 🗑 |
| 2 | 192.168.1.13 | N/A | 1.2.3.6 | N/A | 1-1 | ✎ 🗑 |
| 3 | 192.168.1.1 | 192.168.1.254 | 1.2.3.4 | N/A | M-1 | ✎ 🗑 |
| 4 | ... | ... | ... | ... | - | ✎ 🗑 |
| 5 | ... | ... | ... | ... | - | ✎ 🗑 |
| 6 | ... | ... | ... | ... | - | ✎ 🗑 |
| 7 | ... | ... | ... | ... | - | ✎ 🗑 |
| 8 | ... | ... | ... | ... | - | ✎ 🗑 |
| 9 | ... | ... | ... | ... | - | ✎ 🗑 |
| 10 | ... | ... | ... | ... | - | ✎ 🗑 |

Insert new rule before rule 1 (rule number)

The following table describes the labels in this screen.

**Table 96** ADVANCED > NAT > Address Mapping

| LABEL | DESCRIPTION |
|---|---|
| SUA Address Mapping Rules | This read-only table displays the default address mapping rules. |
| Full Feature Address Mapping Rules | |
| # | This is the rule index number. |
| Local Start IP | This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address. Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types. |
| Global Start IP | This refers to the Inside Global IP Address (IGA), that is the starting global IP address. 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types. |
| Global End IP | This is the ending Inside Global Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types. |

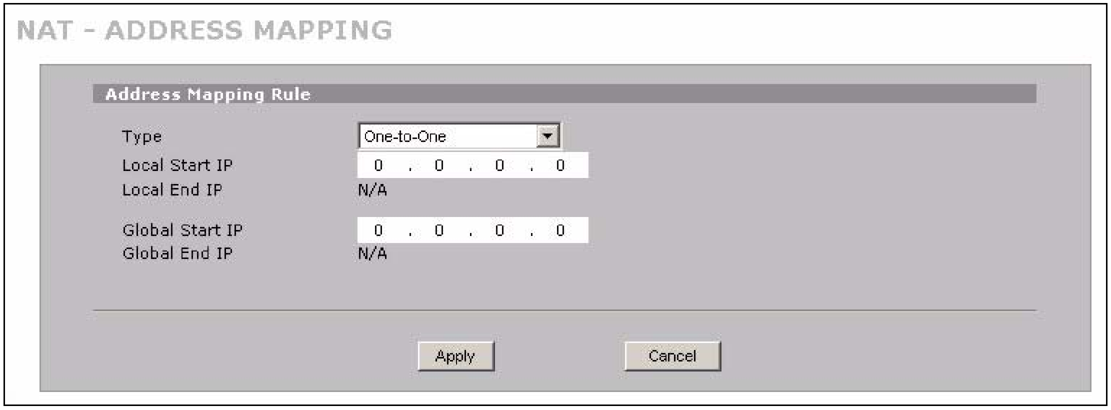
**Table 96** ADVANCED > NAT > Address Mapping (continued)

| LABEL | DESCRIPTION |
|---|---|
| Type | 1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type.<br>2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.<br>3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses.<br>4. **Many One-to-One** mode maps each local IP address to unique global IP addresses.<br>5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Modify | Click the edit icon to go to the screen where you can edit the address mapping rule.<br>Click the delete icon to delete an existing address mapping rule. A window display asking you to confirm that you want to delete the address mapping rule. Note that subsequent address mapping rules move up by one when you take this action. |
| Insert | Click **Insert** to insert a new mapping rule before an existing one. |

## 17.4.2 NAT Address Mapping Edit

Click the edit icon to display the **NAT Address Mapping Edit** screen. Use this screen to edit an address mapping rule. See Section 17.1 on page 331 for information on NAT and address mapping.

**Figure 220** ADVANCED > NAT > Address Mapping > Edit



NAT - ADDRESS MAPPING

Address Mapping Rule

Type: One-to-One
Local Start IP: 0 . 0 . 0 . 0
Local End IP: N/A
Global Start IP: 0 . 0 . 0 . 0
Global End IP: N/A

The following table describes the labels in this screen.

**Table 97** ADVANCED > NAT > Address Mapping > Edit

| LABEL | DESCRIPTION |
|---|---|
| Type | Choose the port mapping type from one of the following.<br>1. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-One NAT mapping type.<br>2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature.<br>3. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.<br>4. **Many One-to-One**: Many One-to-One mode maps each local IP address to unique global IP addresses.<br>5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Local Start IP | This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address.<br>This field is **N/A** for **One-to-One** and **Server** mapping types. |
| Global Start IP | This is the starting Inside Global IP Address (IGA). Enter **0.0.0.0** here if you have a dynamic IP address from your ISP. |
| Global End IP | This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 17.5 Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

### 17.5.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

If you do not assign a Default Server IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

## 17.5.2 Port Forwarding: Services and Port Numbers

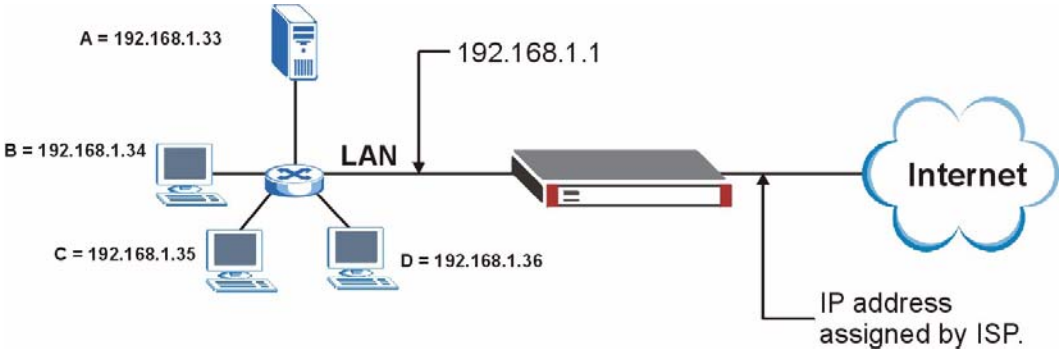
Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network. See Appendix D on page 653 for a list of commonly used services and port numbers.

The ZyWALL provides the additional safety of the DMZ ports for connecting your publicly accessible servers. This makes the LAN more secure by physically separating it from your public servers.

## 17.5.3 Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

**Figure 221** Multiple Servers Behind NAT Example



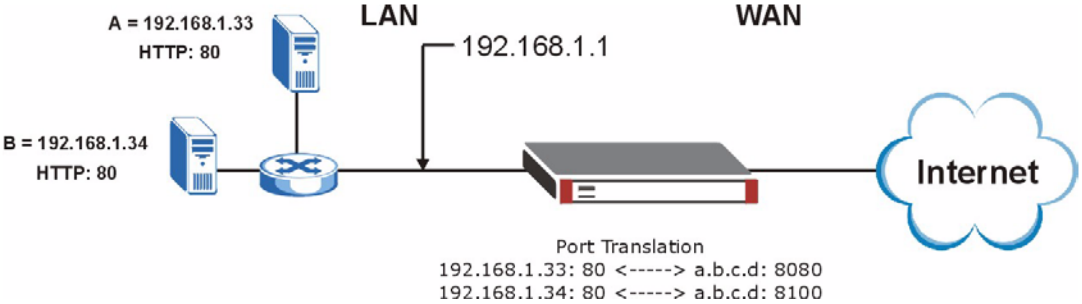
## 17.5.4 Port Translation

The ZyWALL can translate the destination port number or a range of port numbers of packets coming from the WAN to another destination port number or range of port numbers on the local network. When you use port forwarding without port translation, a single server on the local network can use a specific port number and be accessible to the outside world through a single WAN IP address. When you use port translation with port forwarding, multiple servers on the local network can use the same port number and still be accessible to the outside world through a single WAN IP address.

The following example has two web servers on a LAN. Server **A** uses IP address 192.168.1.33 and server **B** uses 192.168.1.34. Both servers use port 80. The letters a.b.c.d represent the WAN port's IP address. The ZyWALL translates port 8080 of traffic received on the WAN port (IP address a.b.c.d) to port 80 and sends it to server **A** (IP address 192.168.1.33). The ZyWALL also translates port 8100 of traffic received on the WAN port (also IP address a.b.c.d) to port 80, but sends it to server **B** (IP address 192.168.1.34).

In this example, anyone wanting to access server A from the Internet must use port 8080. Anyone wanting to access server B from the Internet must use port 8100.

**Figure 222** Port Translation Example



## 17.6 Port Forwarding Screen

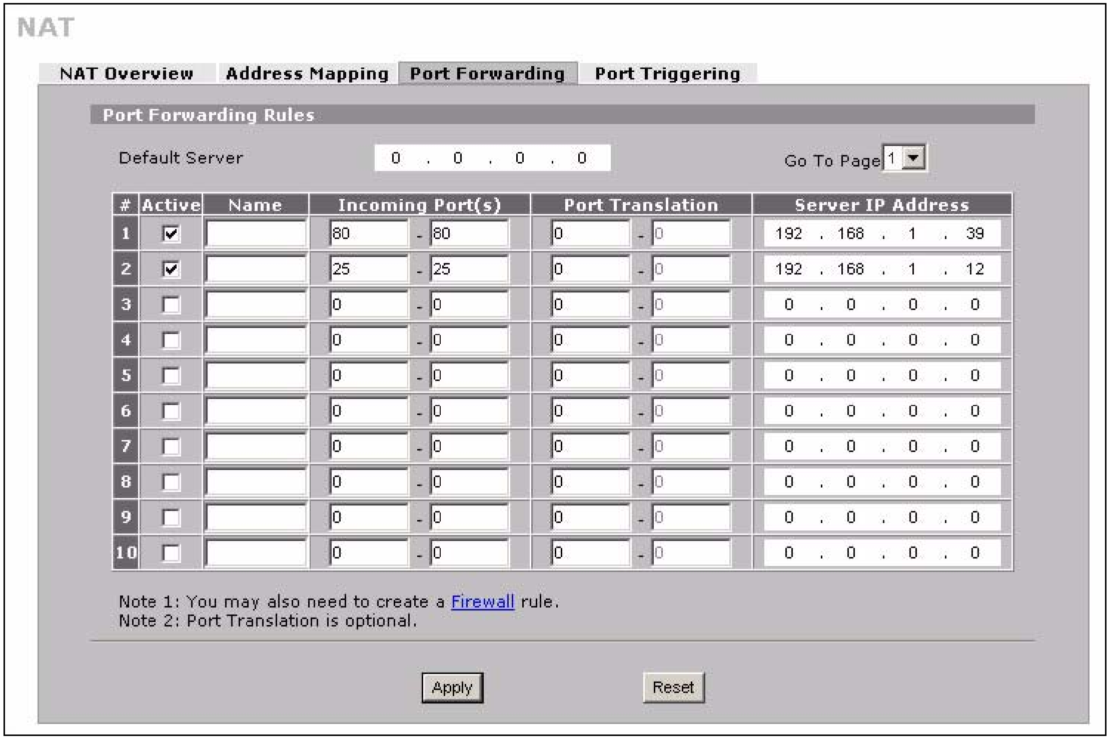
Click **ADVANCED** > **NAT** > **Port Forwarding** to open the **Port Forwarding** screen.

If you do not assign a Default Server IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

Refer to Appendix D on page 653 for port numbers commonly used for particular services.

The last port forwarding rule is reserved for Roadrunner services. The rule is activated only when you set the WAN Encapsulation to Ethernet and the Service Type to something other than Standard.

**Figure 223** ADVANCED > NAT > Port Forwarding



Default Server 0 . 0 . 0 . 0

Go To Page 1

| # | Active | Name | Incoming Port(s) | | Port Translation | | Server IP Address |
|---|---|---|---|---|---|---|---|
| 1 | ☑ | | 80 | 80 | 0 | 0 | 192 . 168 . 1 . 39 |
| 2 | ☑ | | 25 | 25 | 0 | 0 | 192 . 168 . 1 . 12 |
| 3 | ☐ | | 0 | 0 | 0 | 0 | 0 . 0 . 0 . 0 |
| 4 | ☐ | | 0 | 0 | 0 | 0 | 0 . 0 . 0 . 0 |
| 5 | ☐ | | 0 | 0 | 0 | 0 | 0 . 0 . 0 . 0 |
| 6 | ☐ | | 0 | 0 | 0 | 0 | 0 . 0 . 0 . 0 |
| 7 | ☐ | | 0 | 0 | 0 | 0 | 0 . 0 . 0 . 0 |
| 8 | ☐ | | 0 | 0 | 0 | 0 | 0 . 0 . 0 . 0 |
| 9 | ☐ | | 0 | 0 | 0 | 0 | 0 . 0 . 0 . 0 |
| 10 | ☐ | | 0 | 0 | 0 | 0 | 0 . 0 . 0 . 0 |

Note 1: You may also need to create a Firewall rule.
Note 2: Port Translation is optional.

The following table describes the labels in this screen.

**Table 98** ADVANCED > NAT > Port Forwarding

| LABEL | DESCRIPTION |
|---|---|
| Default Server | In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup. |
| Go To Page | Choose a page from the drop-down list box to display the corresponding summary page of the port forwarding servers. |
| # | This is the number of an individual port forwarding server entry. |
| Active | Select this check box to enable the port forwarding server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry. |
| Name | Enter a name to identify this port-forwarding rule. |
| Incoming Port(s) | Enter a port number here. To forward only one port, enter it again in the second field. To specify a range of ports, enter the last port to be forwarded in the second field. |
| Port Translation | Enter the port number here to which you want the ZyWALL to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the ZyWALL automatically calculates the last port of the translated port range. |
| Server IP Address | Enter the inside IP address of the server here. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

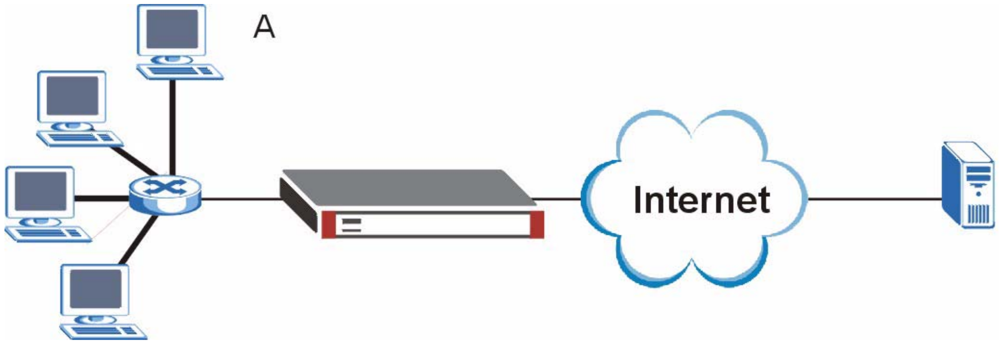
## 17.7 Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

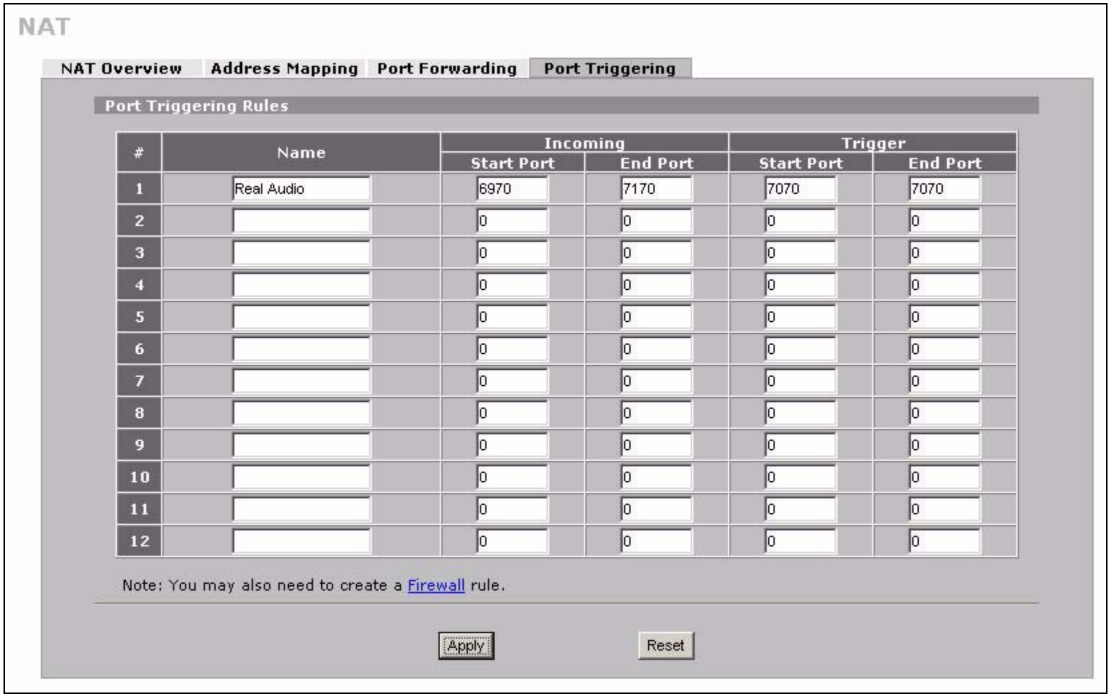
**Figure 224** Trigger Port Forwarding Process: Example



1. Jane (A) requests a file from the Real Audio server (port 7070).
2. Port 7070 is a “trigger” port and causes the ZyWALL to record Jane’s computer IP address. The ZyWALL associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The ZyWALL forwards the traffic to Jane’s computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyWALL times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **ADVANCED** > **NAT** > **Port Triggering** to open the following screen. Use this screen to change your ZyWALL’s trigger port settings.

**Figure 225** ADVANCED > NAT > Port Triggering



| # | Name | Incoming | | Trigger | |
|---|---|---|---|---|---|
| | | Start Port | End Port | Start Port | End Port |
| 1 | Real Audio | 6970 | 7170 | 7070 | 7070 |
| 2 | | 0 | 0 | 0 | 0 |
| 3 | | 0 | 0 | 0 | 0 |
| 4 | | 0 | 0 | 0 | 0 |
| 5 | | 0 | 0 | 0 | 0 |
| 6 | | 0 | 0 | 0 | 0 |
| 7 | | 0 | 0 | 0 | 0 |
| 8 | | 0 | 0 | 0 | 0 |
| 9 | | 0 | 0 | 0 | 0 |
| 10 | | 0 | 0 | 0 | 0 |
| 11 | | 0 | 0 | 0 | 0 |
| 12 | | 0 | 0 | 0 | 0 |

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 99** ADVANCED > NAT > Port Triggering

| LABEL | DESCRIPTION |
|---|---|
| # | This is the rule index number (read-only). |
| Name | Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces. |
| Incoming | Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. |
| Start Port | Type a port number or the starting port number in a range of port numbers. |
| End Port | Type a port number or the ending port number in a range of port numbers. |
| Trigger | The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN. |
| Start Port | Type a port number or the starting port number in a range of port numbers. |
| End Port | Type a port number or the ending port number in a range of port numbers. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 18

# Static Route

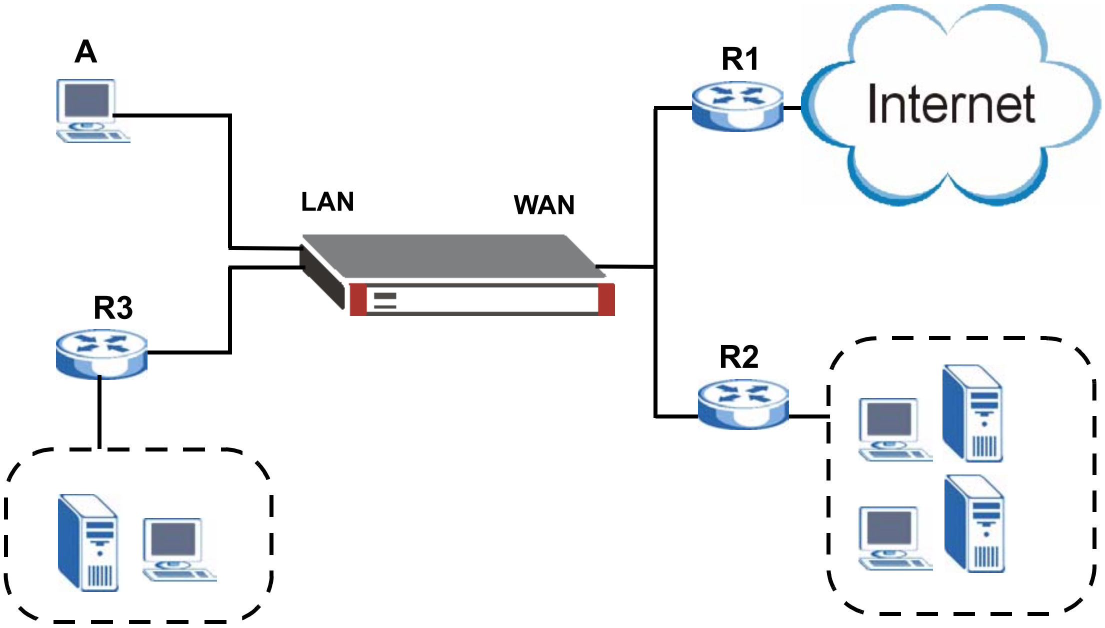
This chapter shows you how to configure static routes for your ZyWALL.

## 18.1 IP Static Route

The ZyWALL usually uses the default gateway to route outbound traffic from local computers to the Internet. To have the ZyWALL send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyWALL's LAN interface. The ZyWALL routes most traffic from **A** to the Internet through the default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router (**R3**) connected to the LAN.

**Figure 226** Example of Static Routing Topology



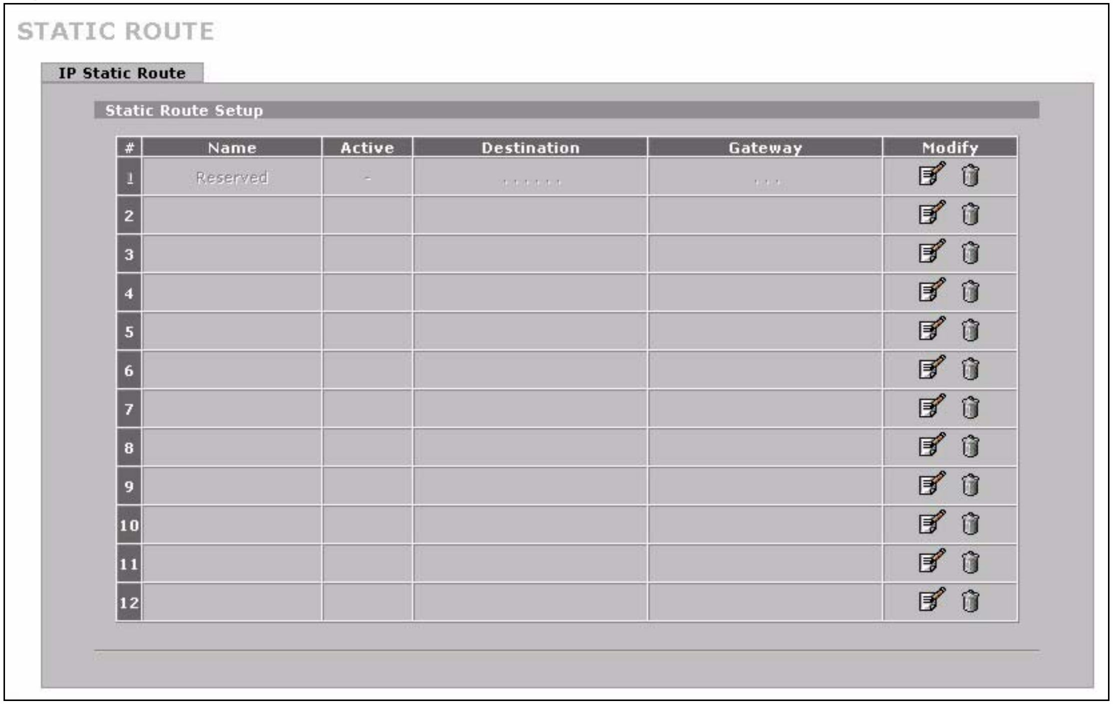
## 18.2 IP Static Route

Click **ADVANCED** > **STATIC ROUTE** to open the **IP Static Route** screen (some of the screen's blank rows are not shown).

The first static route entry is for the default WAN route. You cannot modify or delete a static default route.

The default route is disabled after you change the static WAN IP address to a dynamic WAN IP address.

**Figure 227** ADVANCED > STATIC ROUTE > IP Static Route



| # | Name | Active | Destination | Gateway | Modify |
|---|---|---|---|---|---|
| 1 | Reserved | - | ....... | ... | ✎ 🗑 |
| 2 | | | | | ✎ 🗑 |
| 3 | | | | | ✎ 🗑 |
| 4 | | | | | ✎ 🗑 |
| 5 | | | | | ✎ 🗑 |
| 6 | | | | | ✎ 🗑 |
| 7 | | | | | ✎ 🗑 |
| 8 | | | | | ✎ 🗑 |
| 9 | | | | | ✎ 🗑 |
| 10 | | | | | ✎ 🗑 |
| 11 | | | | | ✎ 🗑 |
| 12 | | | | | ✎ 🗑 |

The following table describes the labels in this screen.

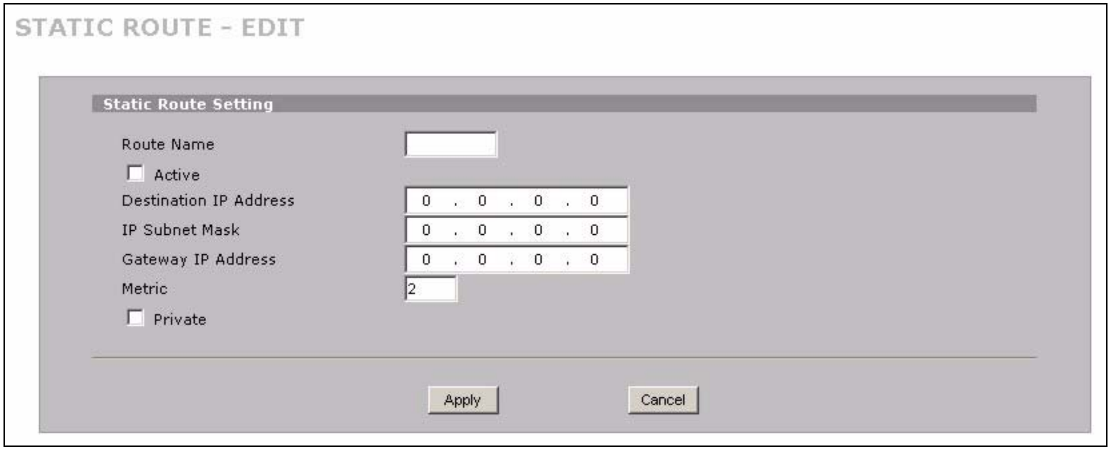
**Table 100** ADVANCED > STATIC ROUTE > IP Static Route

| LABEL | DESCRIPTION |
|---|---|
| # | This is the number of an individual static route. |
| Name | This is the name that describes or identifies this route. |
| Active | This field shows whether this static route is active (**Yes**) or not (**No**). |
| Destination | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Gateway | This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the ZyWALL's interface. The gateway helps forward packets to their destinations. |
| Modify | Click the edit icon to go to the screen where you can set up a static route on the ZyWALL.<br>Click the delete icon to remove a static route from the ZyWALL. A window displays asking you to confirm that you want to delete the route. |

## 18.2.1 IP Static Route Edit

Click the edit icon in the **IP Static Route** screen. The screen shown next appears. Use this screen to configure the required information for a static route.

**Figure 228** ADVANCED > STATIC ROUTE > IP Static Route > Edit



STATIC ROUTE - EDIT

Static Route Setting

Route Name

☐ Active

Destination IP Address 0 . 0 . 0 . 0

IP Subnet Mask 0 . 0 . 0 . 0

Gateway IP Address 0 . 0 . 0 . 0

Metric 2

☐ Private

The following table describes the labels in this screen.

**Table 101** ADVANCED > STATIC ROUTE > IP Static Route > Edit

| LABEL | DESCRIPTION |
|---|---|
| Route Name | Enter the name of the IP static route. Leave this field blank to delete this static route. |
| Active | This field allows you to activate/deactivate this static route. |
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| IP Subnet Mask | Enter the IP subnet mask here. |
| Gateway IP Address | Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Metric | Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number. |
| Private | This parameter determines if the ZyWALL will include this route to a remote node in its RIP broadcasts.<br>Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 19

# Bandwidth Management

This chapter describes the functions and configuration of bandwidth management with multiple levels of sub-classes.

## 19.1 Bandwidth Management Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the ZyWALL forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1024 kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1024 kbps.

## 19.2 Bandwidth Classes and Filters

Use bandwidth classes and sub-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or sub-class) based on a specific application and/or subnet. Use the **Class Setup** screen (see Section 19.12.1 on page 359) to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure sub-classes with filters for any classes that you configure without filters. The ZyWALL leaves the bandwidth budget allocated and unused for a class that does not have a filter or sub-classes with filters. View your configured bandwidth classes and sub-classes in the **Class Setup** screen (see Section 19.12 on page 358 for details).

The total of the configured bandwidth budgets for sub-classes cannot exceed the configured bandwidth budget speed of the parent class.

## 19.3 Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

## 19.4 Application-based Bandwidth Management

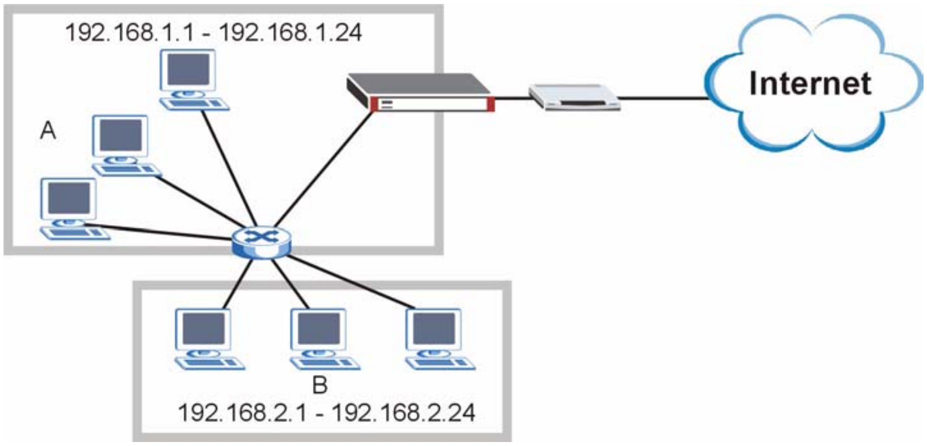
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

## 19.5 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet A and another for subnet B.

**Figure 229** Subnet-based Bandwidth Management Example



## 19.6 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

**Table 102** Application and Subnet-based Bandwidth Management Example

| TRAFFIC TYPE | FROM SUBNET A | FROM SUBNET B |
|---|---|---|
| VoIP | 64 Kbps | 64 Kbps |
| Web | 64 Kbps | 64 Kbps |
| FTP | 64 Kbps | 64 Kbps |

**Table 102** Application and Subnet-based Bandwidth Management Example

| TRAFFIC TYPE | FROM SUBNET A | FROM SUBNET B |
|---|---|---|
| E-mail | 64 Kbps | 64 Kbps |
| Video | 64 Kbps | 64 Kbps |

## 19.7 Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The ZyWALL has two types of scheduler: fairness-based and priority-based.

### 19.7.1 Priority-based Scheduler

With the priority-based scheduler, the ZyWALL forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

### 19.7.2 Fairness-based Scheduler

The ZyWALL divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

### 19.7.3 Maximize Bandwidth Usage

The maximize bandwidth usage option allows the ZyWALL to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyWALL first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the ZyWALL divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the ZyWALL gives extra bandwidth to that class.

When multiple classes require more bandwidth, the ZyWALL gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The ZyWALL distributes the available bandwidth equally among classes with the same priority level.

### 19.7.4 Reserving Bandwidth for Non-Bandwidth Class Traffic

Do the following three steps to configure the ZyWALL to allow bandwidth for traffic that is not defined in a bandwidth filter.

1 Leave some of the interface's bandwidth unbudgeted.

2. Do not enable the interface's **Maximize Bandwidth Usage** option.
3. Do not enable bandwidth borrowing on the sub-classes that have the root class as their parent (see Section 19.8 on page 355).

### 19.7.5 Maximize Bandwidth Usage Example

Here is an example of a ZyWALL that has maximize bandwidth usage enabled on an interface. The following table shows each bandwidth class's bandwidth budget. The classes are set up based on subnets. The interface is set to 10240 kbps. Each subnet is allocated 2048 kbps. The unbudgeted 2048 kbps allows traffic not defined in any of the bandwidth filters to go out when you do not select the maximize bandwidth option.

**Table 103** Maximize Bandwidth Usage Example

| BANDWIDTH CLASSES AND ALLOTMENTS | |
|---|---|
| Root Class: 10240 kbps | Administration: 2048 kbps |
| | Sales: 2048 kbps |
| | Marketing: 2048 kbps |
| | Research: 2048 kbps |

The ZyWALL divides up the unbudgeted 2048 kbps among the classes that require more bandwidth. If the administration department only uses 1024 kbps of the budgeted 2048 kbps, the ZyWALL also divides the remaining 1024 kbps among the classes that require more bandwidth. Therefore, the ZyWALL divides a total of 3072 kbps of unbudgeted and unused bandwidth among the classes that require more bandwidth.

#### 19.7.5.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the priorities of the bandwidth classes and the amount of bandwidth that each class gets.

**Table 104** Priority-based Allotment of Unused and Unbudgeted Bandwidth Example

| BANDWIDTH CLASSES, PRIORITIES AND ALLOTMENTS | |
|---|---|
| Root Class: 10240 kbps | Administration: Priority 4, 1024 kbps |
| | Sales: Priority 6, 3584 kbps |
| | Marketing: Priority 6, 3584 kbps |
| | Research: Priority 5, 2048 kbps |

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The sales and marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1536 kbps or more of extra bandwidth, the ZyWALL divides the total 3072 kbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1536 kbps extra to each for a total of 3584 kbps for each) because they both have the highest priority level.
- Research requires more bandwidth but only gets its budgeted 2048 kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.

#### 19.7.5.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the amount of bandwidth that each class gets.

**Table 105** Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example

| BANDWIDTH CLASSES AND ALLOTMENTS | |
|---|---|
| Root Class: 10240 kbps | Administration: 1024 kbps |
| | Sales: 3072 kbps |
| | Marketing: 3072 kbps |
| | Research: 3072 kbps |

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The ZyWALL divides the total 3072 kbps total of unbudgeted and unused bandwidth equally among the other classes. 1024 kbps extra goes to each so the other classes each get a total of 3072 kbps.

## 19.8 Bandwidth Borrowing

Bandwidth borrowing allows a sub-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows bandwidth classes to borrow any unused or unbudgeted bandwidth on the whole interface.

Enable bandwidth borrowing on a sub-class to allow the sub-class to use its parent class's unused bandwidth. A parent class's unused bandwidth is given to the highest priority sub-class first. The sub-class can also borrow bandwidth from a higher parent class (grandparent class) if the sub-class's parent class is also configured to borrow bandwidth from its parent class. This can go on for as many levels as are configured to borrow bandwidth from their parent class (see Section 19.8.1 on page 355).

The total of the bandwidth allotments for sub-classes cannot exceed the bandwidth allotment of their parent class. The ZyWALL uses the scheduler to divide a parent class's unused bandwidth among the sub-classes.

### 19.8.1 Bandwidth Borrowing Example

Here is an example of bandwidth management with classes configured for bandwidth borrowing. The classes are set up based on departments and individuals within certain departments.

Refer to the product specifications in the appendix to see how many class levels you can configure on your ZyWALL.

**Table 106** Bandwidth Borrowing Example

| BANDWIDTH CLASSES AND BANDWIDTH BORROWING SETTINGS | |
|---|---|
| Root Class: | Administration: Borrowing Enabled |
| | Sales: Borrowing Disabled |
| | Marketing: Borrowing Enabled |
| | Research: Borrowing Enabled |

- The Administration class can borrow unused bandwidth from the Root class because the Administration class has bandwidth borrowing enabled.
- The Sales class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.

## 19.9 Maximize Bandwidth Usage With Bandwidth Borrowing

If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual sub-classes), the ZyWALL functions as follows.

1. The ZyWALL sends traffic according to each bandwidth class's bandwidth budget.
2. The ZyWALL assigns a parent class's unused bandwidth to its sub-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The ZyWALL gives priority to sub-classes of higher priority and treats classes of the same priority equally.
3. The ZyWALL assigns any remaining unused or unbudgeted bandwidth on the interface to any class that requires it. The ZyWALL gives priority to classes of higher priority and treats classes of the same level equally.
4. If the bandwidth requirements of all of the traffic classes are met and there is still some unbudgeted bandwidth, the ZyWALL assigns it to traffic that does not match any of the classes.

## 19.10 Over Allotment of Bandwidth

It is possible to set the bandwidth management speed for an interface higher than the interface's actual transmission speed. Higher priority traffic gets to use up to its allocated bandwidth, even if it takes up all of the interface's available bandwidth. This could stop lower priority traffic from being sent. The following is an example.

**Table 107** Over Allotment of Bandwidth Example

| BANDWIDTH CLASSES, ALLOTMENTS | | PRIORITIES |
|---|---|---|
| Actual outgoing bandwidth available on the interface: 1000 kbps | | |
| Root Class: 1500 kbps (same as Speed setting) | VoIP traffic (Service = SIP): 500 Kbps | 7 |
| | NetMeeting traffic (Service = H.323): 500 kbps | 7 |
| | FTP (Service = FTP): 500 Kbps | 3 |

If you use VoIP and NetMeeting at the same time, the device allocates up to 500 Kbps of bandwidth to each of them before it allocates any bandwidth to FTP. As a result, FTP can only use bandwidth when VoIP and NetMeeting do not use all of their allocated bandwidth.

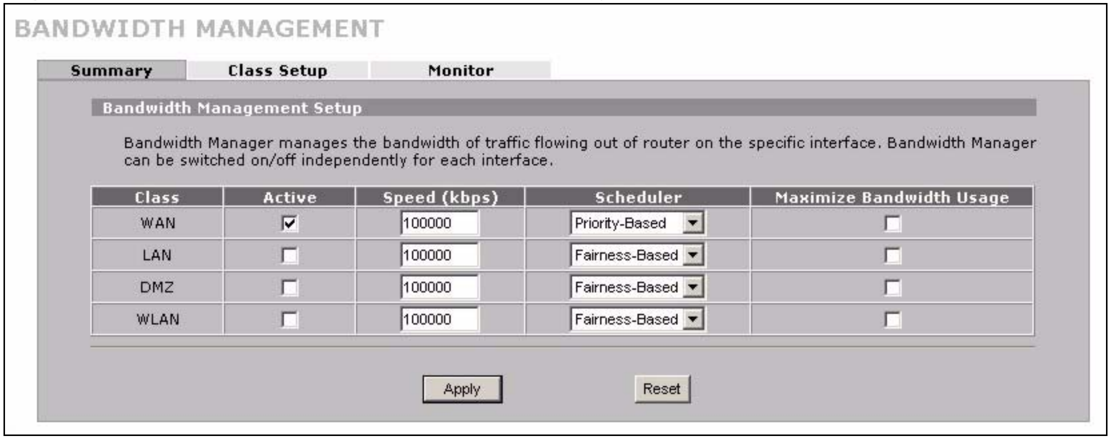
Suppose you try to browse the web too. In this case, VoIP, NetMeeting and FTP all have higher priority, so they get to use the bandwidth first. You can only browse the web when VoIP, NetMeeting, and FTP do not use all 1000 Kbps of available bandwidth.

## 19.11 Configuring Summary

Click **ADVANCED** > **BW MGMT** to open the **Summary** screen.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

**Figure 230** ADVANCED > BW MGMT > Summary



Bandwidth Manager manages the bandwidth of traffic flowing out of router on the specific interface. Bandwidth Manager can be switched on/off independently for each interface.

| Class | Active | Speed (kbps) | Scheduler | Maximize Bandwidth Usage |
|---|---|---|---|---|
| WAN | ☑ | 100000 | Priority-Based | ☐ |
| LAN | ☐ | 100000 | Fairness-Based | ☐ |
| DMZ | ☐ | 100000 | Fairness-Based | ☐ |
| WLAN | ☐ | 100000 | Fairness-Based | ☐ |

The following table describes the labels in this screen.

**Table 108** ADVANCED > BW MGMT > Summary

| LABEL | DESCRIPTION |
|---|---|
| Class | These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source.<br>Traffic redirect or IP alias may cause LAN-to-LAN or DMZ-to-DMZ traffic to pass through the ZyWALL and be managed by bandwidth management. |
| Active | Select an interface's check box to enable bandwidth management on that interface. |
| Speed (kbps) | Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class (see Section 19.12 on page 358).<br>The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 1000 kbps if your Internet connection has an upstream transmission speed of 1 Mbps.<br>You can set this number higher than the interface's actual transmission speed. This will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth.<br>You can also set this number lower than the interface's actual transmission speed. If you do not enable **Maximize Bandwidth Usage**, this will cause the ZyWALL to not use some of the interface's available bandwidth. |

**Table 108** ADVANCED > BW MGMT > Summary (continued)

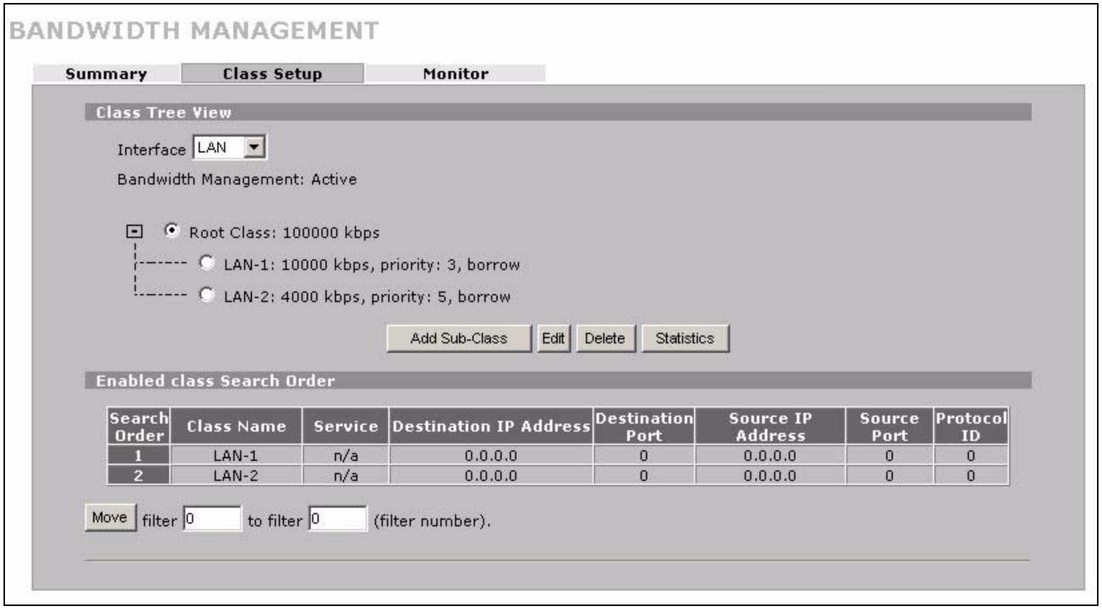
| LABEL | DESCRIPTION |
|---|---|
| Scheduler | Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow.<br>Select **Priority-Based** to give preference to bandwidth classes with higher priorities.<br>Select **Fairness-Based** to treat all bandwidth classes equally. See Section 19.7 on page 353. |
| Maximize Bandwidth Usage | Select this check box to have the ZyWALL divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see Section 19.7.4 on page 353) or you want to limit the speed of this interface (see the **Speed** field description). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 19.12 Configuring Class Setup

The **Class Setup** screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-" to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see Section 19.11 on page 357 to configure the speed of the interface). Configure sub-class layers for the root class.

To add or delete child classes on an interface, click **ADVANCED** > **BW MGMT** > **Class Setup**. The screen is shown here with example classes.

**Figure 231** ADVANCED > BW MGMT > Class Setup



Interface LAN

Bandwidth Management: Active

● Root Class: 100000 kbps

○ LAN-1: 10000 kbps, priority: 3, borrow

○ LAN-2: 4000 kbps, priority: 5, borrow

| Search Order | Class Name | Service | Destination IP Address | Destination Port | Source IP Address | Source Port | Protocol ID |
|---|---|---|---|---|---|---|---|
| 1 | LAN-1 | n/a | 0.0.0.0 | 0 | 0.0.0.0 | 0 | 0 |
| 2 | LAN-2 | n/a | 0.0.0.0 | 0 | 0.0.0.0 | 0 | 0 |

Move filter 0 to filter 0 (filter number).

The following table describes the labels in this screen.

**Table 109** ADVANCED > BW MGMT > Class Setup

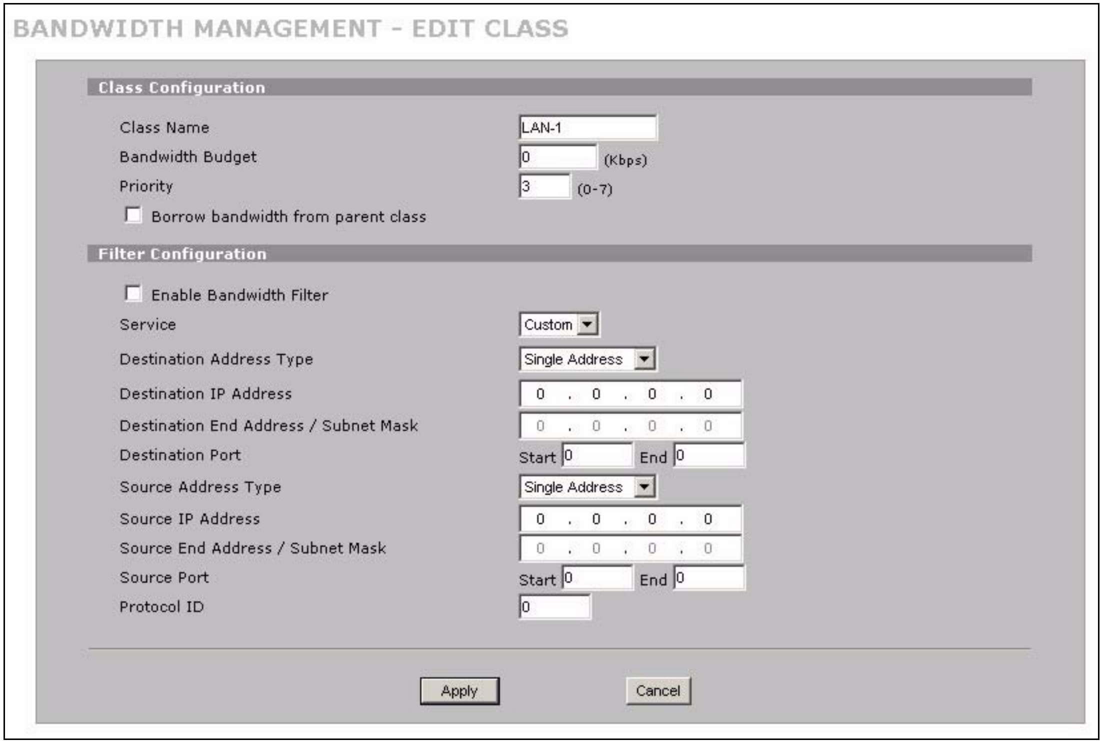
| LABEL | DESCRIPTION |
|---|---|
| Interface | Select an interface for which you want to set up bandwidth management classes.<br>Bandwidth management controls outgoing traffic on an interface, not incoming. So, in order to limit the download bandwidth of the LAN users, set the bandwidth management class on the LAN. In order to limit the upload bandwidth, set the bandwidth management class on the corresponding WAN interface. |
| Bandwidth Management | This field displays whether bandwidth management on the interface you selected in the field above is enabled (**Active**) or not (**Inactive**). |
| | After you select an interface, the bandwidth management classes configured for the interface display. The name and bandwidth display for each class. |
| Add Sub-Class | Click **Add Sub-class** to add a sub-class. |
| Edit | Click **Edit** to configure the selected class. You cannot edit the root class. |
| Delete | Click **Delete** to delete the class and all its sub-classes. You cannot delete the root class. |
| Statistics | Click **Statistics** to display the status of the selected class. |
| Enabled classes Search Order | This list displays the interface's active bandwidth management classes (the ones that have the bandwidth filter enabled). The ZyWALL applies the classes in the order that they appear here. Once a connection matches a bandwidth management class, the ZyWALL applies the class's rules and does not check the connection against any other bandwidth management classes. |
| Search Order | This is the index number of an individual bandwidth management class. |
| Class Name | This is the name that identifies a bandwidth management class. |
| Service | This is the service that this bandwidth management filter is configured to manage. |
| Destination IP Address | This is the destination IP address for connections to which this bandwidth management filter applies. |
| Destination Port | This is the destination port for connections to which this bandwidth management filter applies. |
| Source IP Address | This is the source IP address for connections to which this bandwidth management filter applies. |
| Source Port | This is the source port for connections to which this bandwidth management filter applies. |
| Protocol ID | This is the protocol ID (service type) number for connections to which this bandwidth management filter applies. For example: 1 for ICMP, 6 for TCP or 17 for UDP. |
| Move | Type a filter's index number and the number for where you want to put that filter. Click **Move** to move the filter to the number that you typed. The ordering of your filters is important as they are applied in order of their numbering. |

## 19.12.1 Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Setup** screen. You must use the **Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

Click **ADVANCED** > **BW MGMT** > **Class Setup** > **Add Sub-Class** or **Edit** to open the following screen. Use this screen to add a child class.

**Figure 232** ADVANCED > BW MGMT > Class Setup > Add Sub-Class



BANDWIDTH MANAGEMENT - EDIT CLASS

Class Configuration

Class Name: LAN-1
Bandwidth Budget: 0 (Kbps)
Priority: 3 (0-7)
☐ Borrow bandwidth from parent class

Filter Configuration

☐ Enable Bandwidth Filter
Service: Custom
Destination Address Type: Single Address
Destination IP Address: 0 . 0 . 0 . 0
Destination End Address / Subnet Mask: 0 . 0 . 0 . 0
Destination Port: Start 0 End 0
Source Address Type: Single Address
Source IP Address: 0 . 0 . 0 . 0
Source End Address / Subnet Mask: 0 . 0 . 0 . 0
Source Port: Start 0 End 0
Protocol ID: 0

The following table describes the labels in this screen.

**Table 110** ADVANCED > BW MGMT > Class Setup > Add Sub-Class

| LABEL | DESCRIPTION |
|---|---|
| Class Configuration | |
| Class Name | Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces. |
| Bandwidth Budget (kbps) | Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class. |
| Priority | Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3. |
| Borrow bandwidth from parent class | Select this option to allow a sub-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget.<br>Bandwidth borrowing is governed by the priority of the sub-classes. That is, a sub-class with the highest priority (7) is the first to borrow bandwidth from its parent class.<br>Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types (see Section 19.7.4 on page 353) or you want to set the interface's speed to match what the next device in network can handle (see the **Speed** field description in Table 108 on page 357). |
| Filter Configuration | |
| Enable Bandwidth Filter | Select **Enable Bandwidth Filter** to have the ZyWALL use this bandwidth filter when it performs bandwidth management.<br>You must enter a value in at least one of the following fields (other than the **Subnet Mask** fields which are only available when you enter the destination or source IP address). |

**Table 110** ADVANCED > BW MGMT > Class Setup > Add Sub-Class (continued)

| LABEL | DESCRIPTION |
|---|---|
| Service | This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter).<br>**FTP** (File Transfer Program) is a program to enable fast transfer of files, including large files that may not be possible by e-mail. Select **FTP** from the drop-down list box to configure the bandwidth filter for TCP packets with a port 21 destination.<br>**H.323** is a protocol used for multimedia communications over networks, for example NetMeeting. Select **H.323** from the drop-down list box to configure the bandwidth filter for TCP packets with a port 1720 destination.<br>Note: If you select **H.323**, make sure you also use the **ALG** screen to turn on the H.323 ALG.<br>**SIP** (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification and conferencing. The ZyWALL supports SIP traffic pass-through. Select **SIP** from the drop-down list box to configure this bandwidth filter for UDP packets with a port 5060 destination. This option makes it easier to manage bandwidth for SIP traffic and is useful for example when there is a VoIP (Voice over Internet Protocol) device on your LAN.<br>Note: If you select **SIP**, make sure you also use the **ALG** screen to turn on the SIP ALG.<br>Select **Custom** from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select **Custom**, you need to configure at least one of the following fields (other than the **Subnet Mask** fields which you only enter if you also enter a corresponding destination or source IP address). |
| Destination Address Type | Do you want your rule to apply to packets going to a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50) or a subnet? Select **Single Address, Range Address** or **Subnet Address**. |
| Destination IP Address | Enter the single IP address or the starting IP address in a range here. |
| Destination End Address / Subnet Mask | If you are configuring a range of IP addresses, enter the ending IP address here. If you are configuring a subnet of addresses, enter the subnet mask here. Refer to Appendix C on page 645 for more information on IP subnetting. |
| Destination Port | Enter the starting and ending destination port numbers. Enter the same port number in both fields to specify a single port number. See the following table for some common services and port numbers. |
| Source Address Type | Do you want your rule to apply to packets coming from a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50) or a subnet? Select **Single Address, Range Address** or **Subnet Address**. |
| Source IP Address | Enter the single IP address or the starting IP address in a range here. |
| Source End Address / Subnet Mask | If you are configuring a range of IP addresses, enter the ending IP address here. If you are configuring a subnet of addresses, enter the subnet mask here. Refer to Appendix C on page 645 for more information on IP subnetting. |
| Source Port | Enter the starting and ending destination port numbers. Enter the same port number in both fields to specify a single port number. See the following table for some common services and port numbers. |

**Table 110** ADVANCED > BW MGMT > Class Setup > Add Sub-Class (continued)

| LABEL | DESCRIPTION |
|---|---|
| Protocol ID | Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

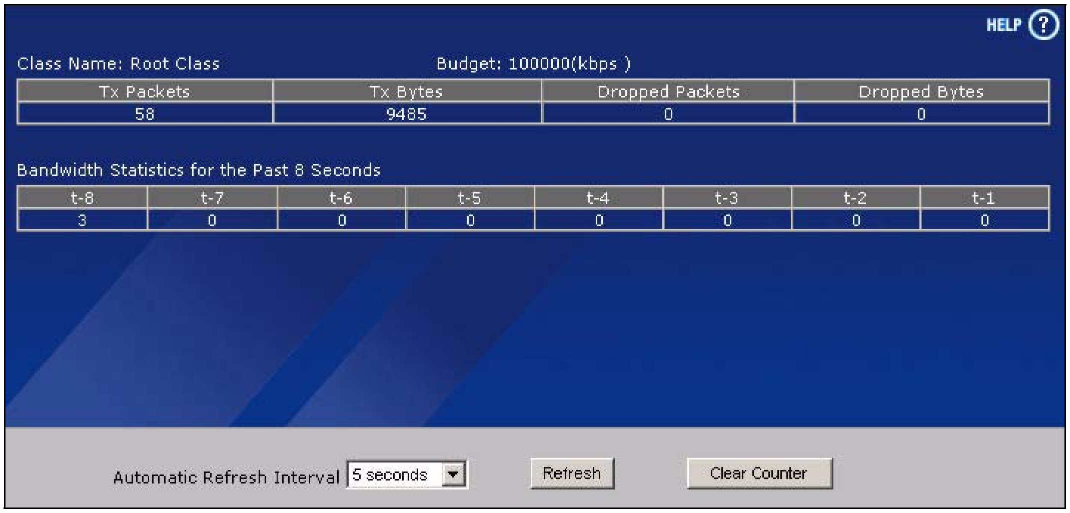
**Table 111** Services and Port Numbers

| SERVICES | PORT NUMBER |
|---|---|
| ECHO | 7 |
| FTP (File Transfer Protocol) | 21 |
| SMTP (Simple Mail Transfer Protocol) | 25 |
| DNS (Domain Name System) | 53 |
| Finger | 79 |
| HTTP (Hyper Text Transfer protocol or WWW, Web) | 80 |
| POP3 (Post Office Protocol) | 110 |
| NNTP (Network News Transport Protocol) | 119 |
| SNMP (Simple Network Management Protocol) | 161 |
| SNMP trap | 162 |
| PPTP (Point-to-Point Tunneling Protocol) | 1723 |

## 19.12.2 Bandwidth Management Statistics

Click **ADVANCED** > **BW MGMT** > **Class Setup** > **Statistics** to open the **Bandwidth Management Statistics** screen. This screen displays the selected bandwidth class's bandwidth usage and allotments.

**Figure 233** ADVANCED > BW MGMT > Class Setup > Statistics



Class Name: Root Class

Budget: 100000(kbps )

| Tx Packets | Tx Bytes | Dropped Packets | Dropped Bytes |
|---|---|---|---|
| 58 | 9485 | 0 | 0 |

Bandwidth Statistics for the Past 8 Seconds

| t-8 | t-7 | t-6 | t-5 | t-4 | t-3 | t-2 | t-1 |
|---|---|---|---|---|---|---|---|
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Automatic Refresh Interval: 5 seconds

The following table describes the labels in this screen.

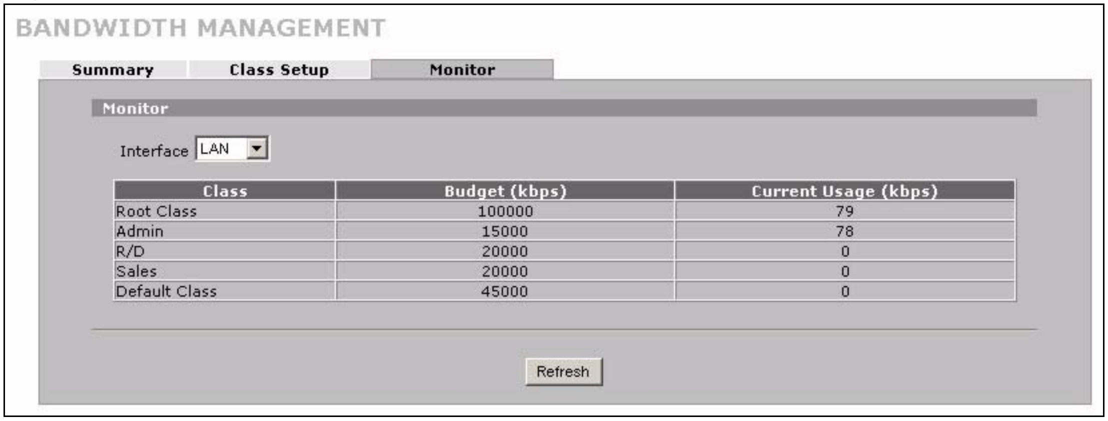
**Table 112** ADVANCED > BW MGMT > Class Setup > Statistics

| LABEL | DESCRIPTION |
|---|---|
| Class Name | This field displays the name of the class the statistics page is showing. |
| Budget (kbps) | This field displays the amount of bandwidth allocated to the class. |
| Tx Packets | This field displays the total number of packets transmitted. |
| Tx Bytes | This field displays the total number of bytes transmitted. |
| Dropped Packets | This field displays the total number of packets dropped. |
| Dropped Bytes | This field displays the total number of bytes dropped. |
| Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1) | |
| This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago. | |
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |
| Clear Counter | Click **Clear Counter** to clear all of the bandwidth management statistics. |

## 19.13 Bandwidth Manager Monitor

Click **ADVANCED** > **BW MGMT** > **Monitor** to open the following screen. Use this screen to view the device's bandwidth usage and allotments.

**Figure 234** ADVANCED > BW MGMT > Monitor



Interface LAN

| Class | Budget (kbps) | Current Usage (kbps) |
|---|---|---|
| Root Class | 100000 | 79 |
| Admin | 15000 | 78 |
| R/D | 20000 | 0 |
| Sales | 20000 | 0 |
| Default Class | 45000 | 0 |

The following table describes the labels in this screen.

**Table 113** ADVANCED > BW MGMT > Monitor

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes. |
| Class | This field displays the name of the bandwidth class.<br>A **Default Class** automatically displays for all the bandwidth in the **Root Class** that is not allocated to bandwidth classes. If you do not enable maximize bandwidth usage on an interface, the ZyWALL uses the bandwidth in this default class to send traffic that does not match any of the bandwidth classes.[A] |
| Budget (kbps) | This field displays the amount of bandwidth allocated to the bandwidth class. |
| Current Usage (kbps) | This field displays the amount of bandwidth that each bandwidth class is using. |
| Refresh | Click **Refresh** to update the page. |

[A] If you allocate all the root class's bandwidth to the bandwidth classes, the default class still displays a budget of 2 kbps (the minimum amount of bandwidth that can be assigned to a bandwidth class).

# 20

# DNS

This chapter shows you how to configure the DNS screens.

## 20.1 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The ZyWALL uses a system DNS server (in the order you specify in the **DNS System** screen) to resolve domain names, for example, VPN, DDNS and the time server.

## 20.2 DNS Server Address Assignment

The ZyWALL can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
3. You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Section 20.5.1 on page 366).

## 20.3 DNS Servers

There are three places where you can configure DNS setup on the ZyWALL.

1. Use the **DNS System** screen to configure the ZyWALL to use a DNS server to resolve domain names for ZyWALL system features like VPN, DDNS and the time server.
2. Use the **DNS DHCP** screen to configure the DNS server information that the ZyWALL sends to the DHCP client devices on the LAN, DMZ or WLAN.
3. Use the **REMOTE MGMT DNS** screen to configure the ZyWALL (in router mode) to accept or discard DNS queries.

## 20.4 Address Record

An address record contains the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com.tw” is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where "mail" is the host, "myZyXEL" is the second-level domain, and "com.tw" is the top level domain.

The ZyWALL allows you to configure address records about the ZyWALL itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the ZyWALL receives a DNS query for an FQDN for which the ZyWALL has an address record, the ZyWALL can send the IP address in a DNS response without having to query a DNS name server.

### 20.4.1 DNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.com to be aliased to the same IP address as yourhost.com. This feature is useful if you want to be able to use, for example, www.yourhost.com and still reach your hostname.

## 20.5 Name Server Record

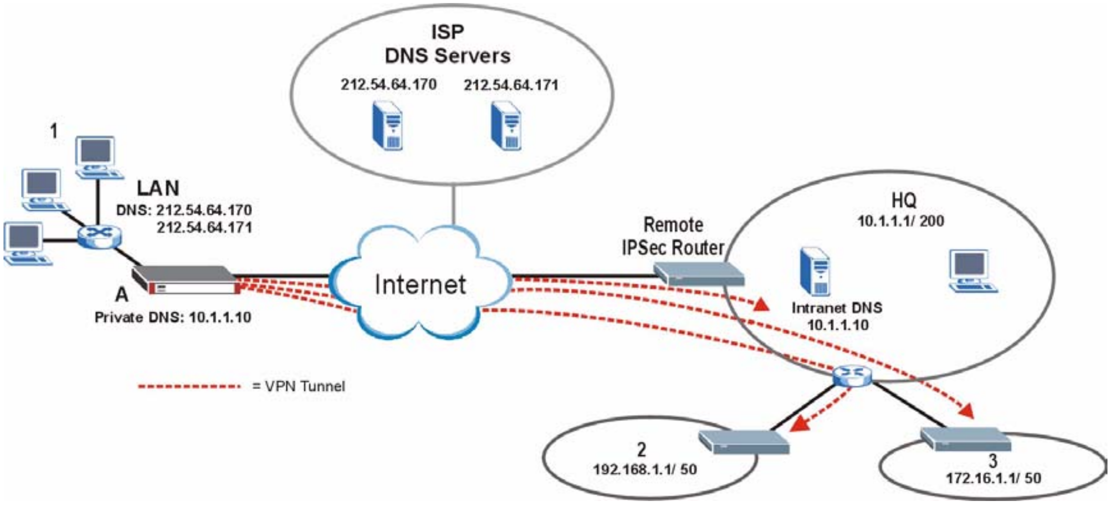
A name server record contains a DNS server’s IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. A domain zone may also be included. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

### 20.5.1 Private DNS Server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

The following figure depicts an example where three VPN tunnels are created from ZyWALL A; one to branch office **2**, one to branch office **3** and another to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the ZyWALL at branch office **1** uses the Intranet DNS server in headquarters.

**Figure 235** Private DNS Server Example

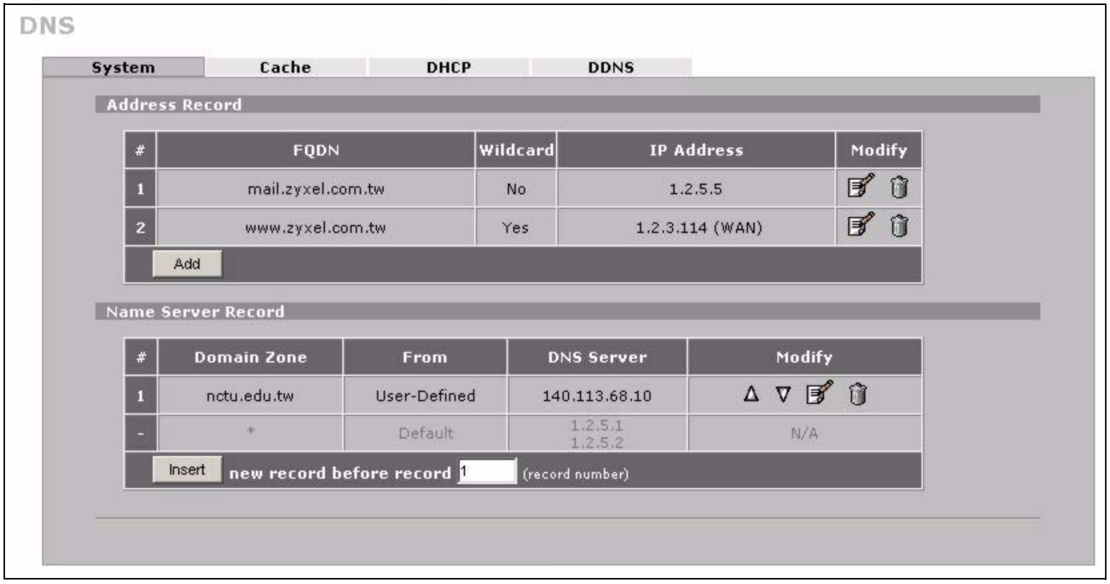

ISP
DNS Servers
212.54.64.170
212.54.64.171
1
LAN
DNS: 212.54.64.170
212.54.64.171
A
Private DNS: 10.1.1.10
Internet
Remote
IPSec Router
HQ
10.1.1.1/ 200
Intranet DNS
10.1.1.10
= VPN Tunnel
2
192.168.1.1/ 50
3
172.16.1.1/ 50

If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

## 20.6 System Screen

Click **ADVANCED** > **DNS** to display the following screen. Use this screen to configure your ZyWALL's DNS address and name server records.

**Figure 236** ADVANCED > DNS > System DNS


DNS
System
Cache
DHCP
DDNS

Address Record

| # | FQDN | Wildcard | IP Address | Modify |
|---|---|---|---|---|
| 1 | mail.zyxel.com.tw | No | 1.2.5.5 | |
| 2 | www.zyxel.com.tw | Yes | 1.2.3.114 (WAN) | |

Add

Name Server Record

| # | Domain Zone | From | DNS Server | Modify |
|---|---|---|---|---|
| 1 | nctu.edu.tw | User-Defined | 140.113.68.10 | Δ ∇ |
| - | * | Default | 1.2.5.1<br>1.2.5.2 | N/A |

Insert new record before record 1 (record number)

The following table describes the labels in this screen.

**Table 114** ADVANCED > DNS > System DNS

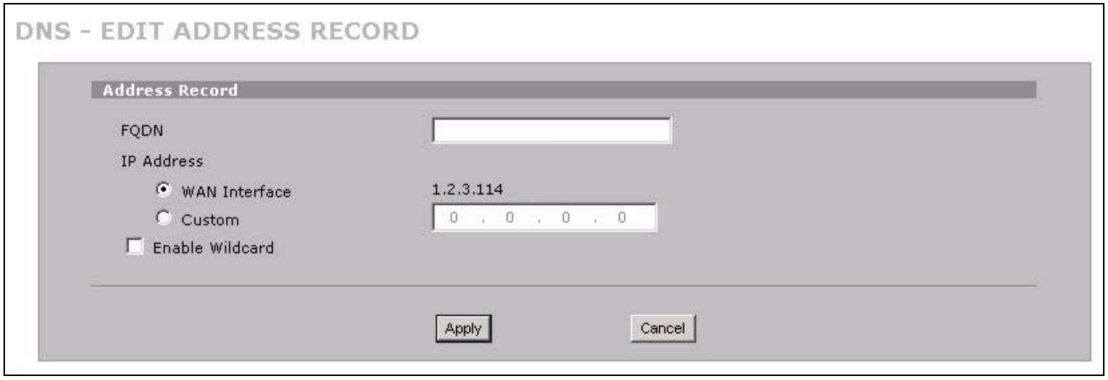
| LABEL | DESCRIPTION |
|---|---|
| Address Record | An address record specifies the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com.tw" is the top level domain. |
| # | This is the index number of the address record. |
| FQDN | This is a host's fully qualified domain name. |
| Wildcard | This column displays whether or not the DNS wildcard feature is enabled for this domain name. |
| IP Address | This is the IP address of a host. |
| Modify | Click the edit icon to go to the screen where you can edit the record.<br>Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action. |
| Add | Click **Add** to open a screen where you can add a new address record. Refer to Table 115 on page 369 for information on the fields. |
| Name Server Record | A name server record contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server.<br>When the ZyWALL needs to resolve a domain name, it checks it against the name server record entries in the order that they appear in this list.<br>A "*" indicates a name server record without a domain zone. The default record is grayed out. The ZyWALL uses this default record if the domain name that needs to be resolved does not match any of the other name server records.<br>A name server record with a domain zone is always put before a record without a domain zone. |
| # | This is the index number of the name server record. |
| Domain Zone | A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. |
| From | This field displays whether the IP address of a DNS server is from a WAN interface (and which it is) or specified by the user. |
| DNS Server | This is the IP address of a DNS server. |
| Modify | Click a triangle icon to move the record up or down in the list.<br>Click the edit icon to go to the screen where you can edit the record.<br>Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action. |
| Insert | Enter the rule number where you want to put the record and click **Insert** to open a screen where you can configure a new name server record. Refer to Table 116 on page 370 for information on the fields. |

## 20.6.1 Adding an Address Record

Click **Add** in the **System** screen to open this screen. Use this screen to add an address record.

An address record contains the mapping of a fully qualified domain name (FQDN) to an IP address. Configure address records about the ZyWALL itself or another device to keep a record of DNS names and addresses that people on your network may use frequently. If the ZyWALL receives a DNS query for an FQDN for which the ZyWALL has an address record, the ZyWALL can send the IP address in a DNS response without having to query a DNS name server. See Section 20.4 on page 366 for more on address records.

**Figure 237** ADVANCED > DNS > Add (Address Record)



WAN Interface: 1.2.3.114

Custom: 0 . 0 . 0 . 0

The following table describes the labels in this screen.

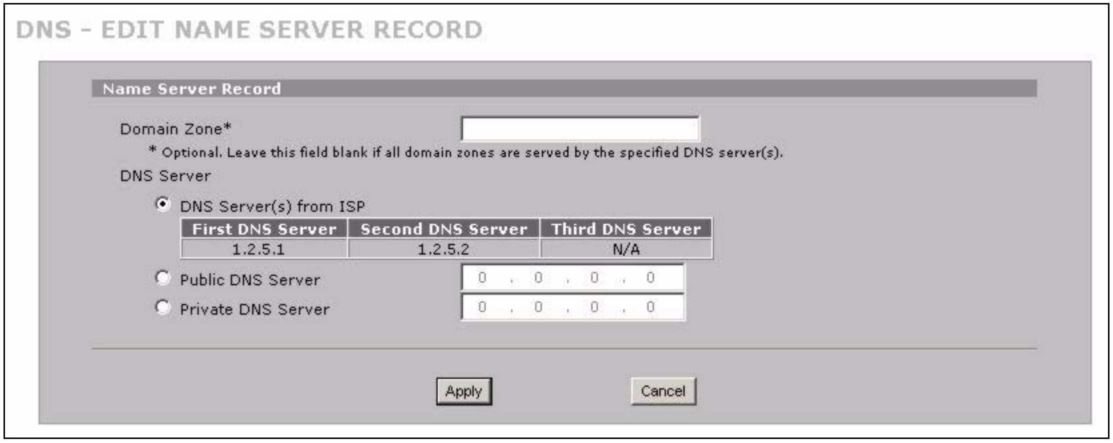
**Table 115** ADVANCED > DNS > Add (Address Record)

| LABEL | DESCRIPTION |
|---|---|
| FQDN | Type a fully qualified domain name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com.tw" is the top level domain. |
| IP Address | If this entry is for the WAN port on the ZyWALL, select **WAN Interface**.<br>For entries that are not for the WAN port, select **Custom** and enter the IP address of the host in dotted decimal notation. |
| Enable Wildcard | Select the check box to enable DNS wildcard. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 20.6.2 Inserting a Name Server Record

Click **Insert** in the **System** screen to open this screen. Use this screen to insert a name server record. A name server record contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. A domain zone may also be included. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

**Figure 238** ADVANCED > DNS > Insert (Name Server Record)



DNS - EDIT NAME SERVER RECORD

Name Server Record

Domain Zone*

* Optional. Leave this field blank if all domain zones are served by the specified DNS server(s).

DNS Server

● DNS Server(s) from ISP

| First DNS Server | Second DNS Server | Third DNS Server |
|---|---|---|
| 1.2.5.1 | 1.2.5.2 | N/A |

○ Public DNS Server 0 . 0 . 0 . 0

○ Private DNS Server 0 . 0 . 0 . 0

The following table describes the labels in this screen.

**Table 116** ADVANCED > DNS > Insert (Name Server Record)

| LABEL | DESCRIPTION |
|---|---|
| Domain Zone | This field is optional.<br>A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ZyWALL receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address.<br>Leave this field blank if all domain zones are served by the specified DNS server(s). |
| DNS Server | Select the **DNS Server(s) from ISP** radio button if your ISP dynamically assigns DNS server information. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address. **N/A** displays for all of the DNS server IP address fields if the ZyWALL has a fixed WAN IP address.<br>Select **Public DNS Server** if you have the IP address of a DNS server. The IP address must be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right.<br>**Public DNS Server** entries with the IP address set to 0.0.0.0 are not allowed.<br>Select **Private DNS Server** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right.<br>With a private DNS server, you must also configure the first DNS server entry for the LAN, DMZ and/or WLAN in the **DNS DHCP** screen to use **DNS Relay**.<br>You must also configure a VPN rule since the ZyWALL uses a VPN tunnel when it relays DNS queries to the private DNS server. The rule must include the LAN IP address of the ZyWALL as a local IP address and the IP address of the DNS server as a remote IP address.<br>**Private DNS Server** entries with the IP address set to 0.0.0.0 are not allowed. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 20.7 DNS Cache

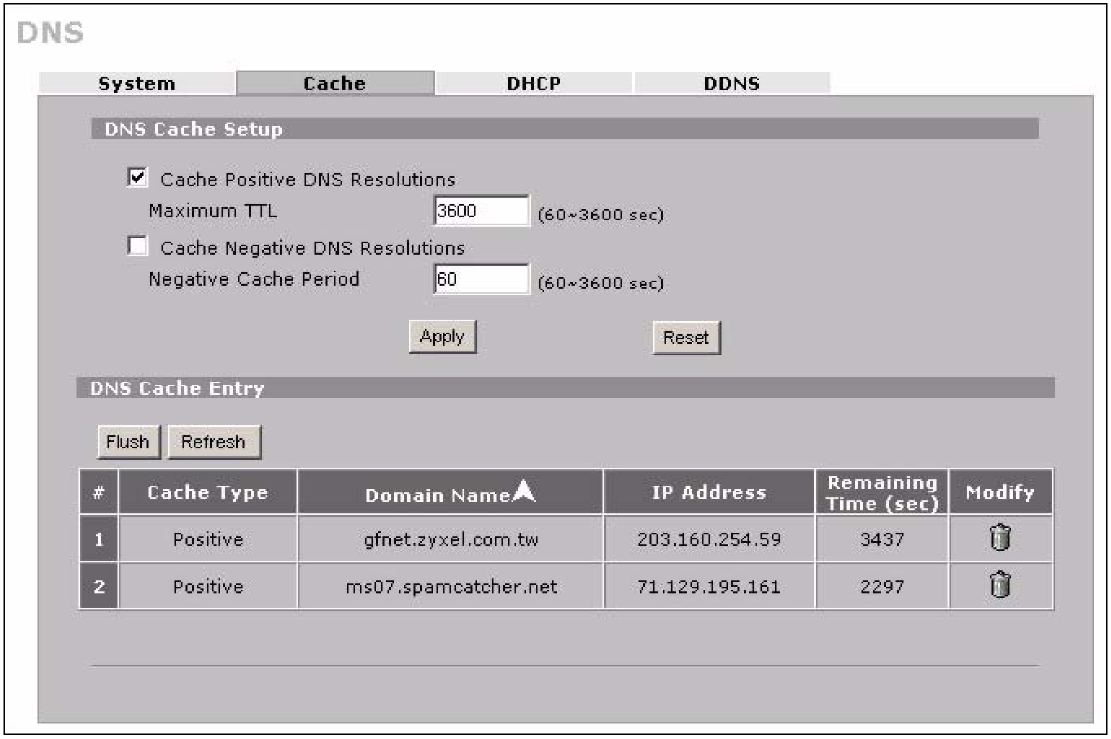
DNS cache is the temporary storage area where a router stores responses from DNS servers. When the ZyWALL receives a positive or negative response for a DNS query, it records the response in the DNS cache. A positive response means that the ZyWALL received the IP address for a domain name that it checked with a DNS server within the five second DNS timeout period. A negative response means that the ZyWALL did not receive a response for a query it sent to a DNS server within the five second DNS timeout period.

When the ZyWALL receives DNS queries, it compares them against the DNS cache before querying a DNS server. If the DNS query matches a positive entry, the ZyWALL responses with the IP address from the entry. If the DNS query matches a negative entry, the ZyWALL replies that the DNS query failed.

## 20.8 Configure DNS Cache

To configure your ZyWALL's DNS caching, click **ADVANCED** > **DNS** > **Cache**. The screen appears as shown.

**Figure 239** ADVANCED > DNS > Cache



☑ Cache Positive DNS Resolutions
Maximum TTL 3600 (60~3600 sec)
☐ Cache Negative DNS Resolutions
Negative Cache Period 60 (60~3600 sec)

| # | Cache Type | Domain Name | IP Address | Remaining Time (sec) | Modify |
|---|---|---|---|---|---|
| 1 | Positive | gfnet.zyxel.com.tw | 203.160.254.59 | 3437 | 🗑 |
| 2 | Positive | ms07.spamcatcher.net | 71.129.195.161 | 2297 | 🗑 |

The following table describes the labels in this screen.

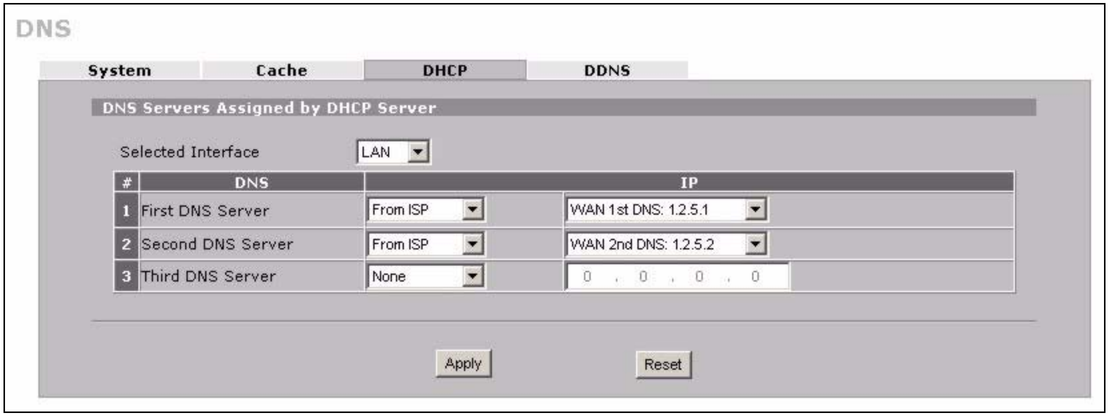
**Table 117** ADVANCED > DNS > Cache

| LABEL | DESCRIPTION |
|---|---|
| DNS Cache Setup | |
| Cache Positive DNS Resolutions | Select the check box to record the positive DNS resolutions in the cache. Caching positive DNS resolutions helps speed up the ZyWALL's processing of commonly queried domain names and reduces the amount of traffic that the ZyWALL sends out to the WAN. |
| Maximum TTL | Type the maximum time to live (TTL) (60 to 3600 seconds). This sets how long the ZyWALL is to allow a positive resolution entry to remain in the DNS cache before discarding it. |
| Cache Negative DNS Resolutions | Caching negative DNS resolutions helps speed up the ZyWALL's processing of commonly queried domain names (for which DNS resolution has failed) and reduces the amount of traffic that the ZyWALL sends out to the WAN. |
| Negative Cache Period | Type the time (60 to 3600 seconds) that the ZyWALL is to allow a negative resolution entry to remain in the DNS cache before discarding it. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| DNS Cache Entry | |
| Flush | Click this button to clear the cache manually. After you flush the cache, the ZyWALL must query the DNS servers again for any domain names that had been previously resolved. |
| Refresh | Click this button to reload the cache. |
| # | This is the index number of a record. |
| Cache Type | This displays whether the response for the DNS request is positive or negative. |
| Domain Name | This is the domain name of a host. |
| IP Address | This is the (resolved) IP address of a host. This field displays **0.0.0.0** for negative DNS resolution entries. |
| Remaining Time (sec) | This is the number of seconds left before the DNS resolution entry is discarded from the cache. |
| Modify | Click the delete icon to remove the DNS resolution entry from the cache. |

## 20.9 Configuring DNS DHCP

Click **ADVANCED** > **DNS** > **DHCP** to open the **DNS DHCP** screen shown next. Use this screen to configure the DNS server information that the ZyWALL sends to its LAN, DMZ or WLAN DHCP clients.

**Figure 240** ADVANCED > DNS > DHCP



DNS Servers Assigned by DHCP Server

Selected Interface: LAN

| # | DNS | IP | |
|---|---|---|---|
| 1 | First DNS Server | From ISP | WAN 1st DNS: 1.2.5.1 |
| 2 | Second DNS Server | From ISP | WAN 2nd DNS: 1.2.5.2 |
| 3 | Third DNS Server | None | 0 . 0 . 0 . 0 |

The following table describes the labels in this screen.

**Table 118** ADVANCED > DNS > DHCP

| LABEL | DESCRIPTION |
|---|---|
| DNS Servers Assigned by DHCP Server | The ZyWALL passes a DNS (Domain Name System) server IP address to the DHCP clients. |
| Selected Interface | Select an interface from the drop-down list box to configure the DNS servers for the specified interface. |
| DNS | These read-only labels represent the DNS servers. |
| IP | Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyWALL's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right.<br>Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**.<br>Select **DNS Relay** to have the ZyWALL act as a DNS proxy. The ZyWALL's LAN, DMZ or WLAN IP address displays in the field to the right (read-only). The ZyWALL tells the DHCP clients on the LAN, DMZ or WLAN that the ZyWALL itself is the DNS server. When a computer on the LAN, DMZ or WLAN sends a DNS query to the ZyWALL, the ZyWALL forwards the query to the ZyWALL's system DNS server (configured in the **DNS System** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to **None** after you click **Apply**.<br>Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 20.10 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

You must go to the Dynamic DNS service provider’s website and register a user account and a domain name before you can use the Dynamic DNS service with your ZyWALL.

### 20.10.1 DYNDNS Wildcard

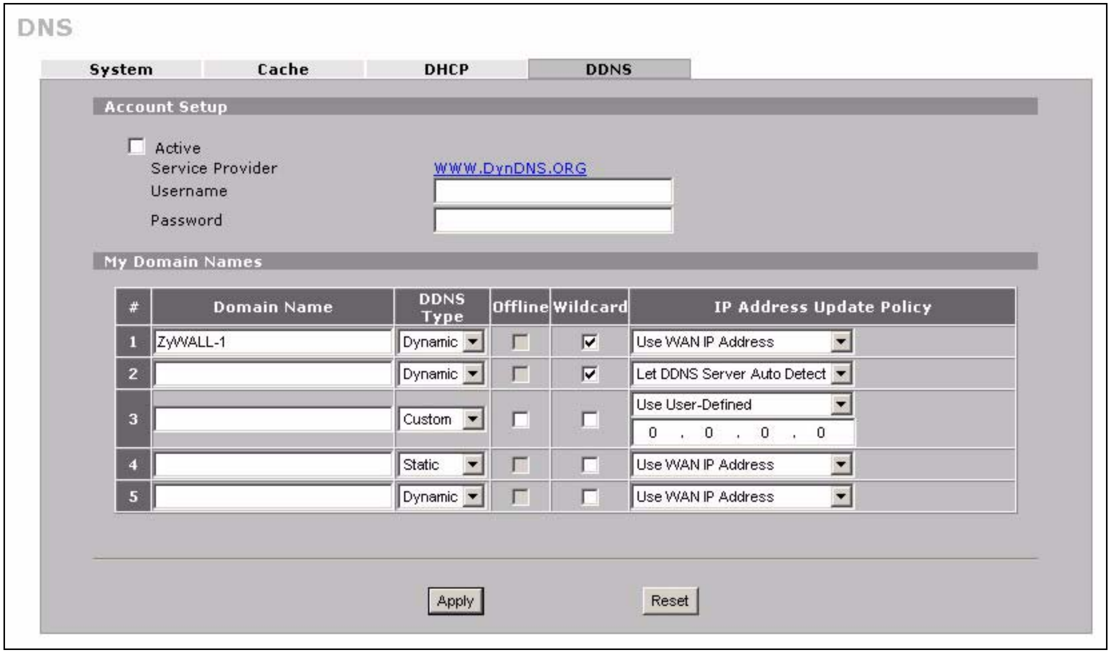
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

## 20.11 Configuring Dynamic DNS

To change your ZyWALL’s DDNS, click **ADVANCED** > **DNS** > **DDNS**. The screen appears as shown.

**Figure 241** ADVANCED > DNS > DDNS



☐ Active
Service Provider WWW.DynDNS.ORG
Username
Password

| # | Domain Name | DDNS Type | Offline | Wildcard | IP Address Update Policy |
|---|---|---|---|---|---|
| 1 | ZyWALL-1 | Dynamic | ☐ | ☑ | Use WAN IP Address |
| 2 | | Dynamic | ☐ | ☑ | Let DDNS Server Auto Detect |
| 3 | | Custom | ☐ | ☐ | Use User-Defined<br>0 . 0 . 0 . 0 |
| 4 | | Static | ☐ | ☐ | Use WAN IP Address |
| 5 | | Dynamic | ☐ | ☐ | Use WAN IP Address |

The following table describes the labels in this screen.

**Table 119** ADVANCED > DNS > DDNS

| LABEL | DESCRIPTION |
|---|---|
| Account Setup | |
| Active | Select this check box to use dynamic DNS. |
| Service Provider | This is the name of your Dynamic DNS service provider. |
| Username | Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Password | Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed. |
| My Domain Names | |
| Domain Name 1~5 | Enter the host names in these fields. |
| DDNS Type | Select the type of service that you are registered for from your Dynamic DNS service provider.<br>Select **Dynamic** if you have the Dynamic DNS service.<br>Select **Static** if you have the Static DNS service.<br>Select **Custom** if you have the Custom DNS service. |
| Offline | This option is available when **Custom** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line. |
| Wildcard | Select the check box to enable DYNDNS Wildcard. |

**Table 119** ADVANCED > DNS > DDNS

| LABEL | DESCRIPTION |
|---|---|
| IP Address Update Policy | Select **Use WAN IP Address** to have the ZyWALL update the domain name with the WAN port's IP address.<br>Select **Use User-Defined** and enter the IP address if you have a static IP address.<br>Select **Let DDNS Server Auto Detect** only when there are one or more NAT routers between the ZyWALL and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.<br>Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 21

# Remote Management

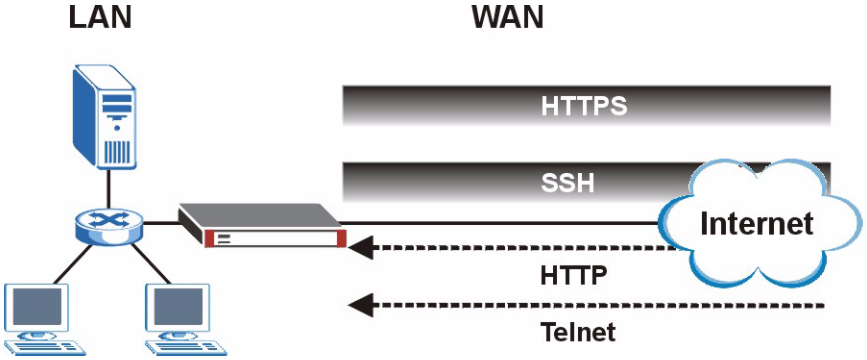
This chapter provides information on the Remote Management screens.

## 21.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyWALL interface (if any) from which computers.

The following figure shows secure and insecure management of the ZyWALL coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

**Figure 242** Secure and Insecure Remote Management From the WAN



When you configure remote management to allow management from any network except the LAN, you still need to configure a firewall rule to allow access. See Chapter 11 on page 191 for details on configuring firewall rules.

You can also disable a service on the ZyWALL by not allowing access for the service/protocol through any of the ZyWALL interfaces.

You may only have one remote management session running at a time. The ZyWALL automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Console port
2. SSH

3. Telnet
4. HTTPS and HTTP

### 21.1.1 Remote Management Limitations

Remote management does not work when:

1. You have not enabled that service on the interface in the corresponding remote management screen.
2. You have disabled that service in one of the remote management screens.
3. The IP address in the **Secure Client IP Address** field does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
4. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
5. There is a firewall rule that blocks it.
6. A filter is applied (through the SMT or the commands) to block a Telnet, FTP or Web service.

### 21.1.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyWALL automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **MAINTENANCE > General** screen.

## 21.2 WWW (HTTP and HTTPS)

You can set the ZyWALL to use HTTP or HTTPS (HTTPS adds security) for web configurator sessions. Specify which interfaces allow web configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

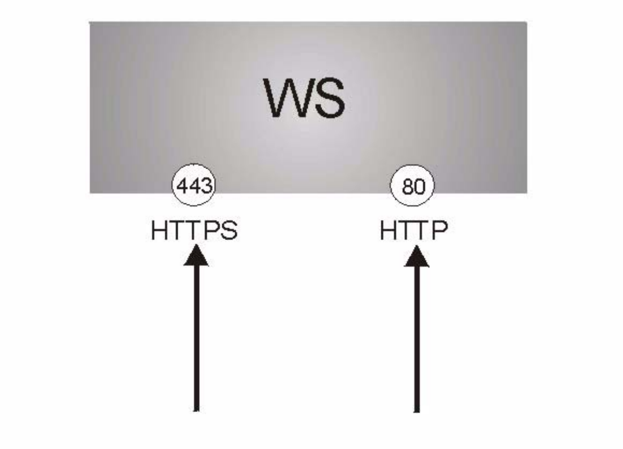
It relies upon certificates, public keys, and private keys (see Chapter 15 on page 295 for more information).

HTTPS on the ZyWALL is used so that you may securely access the ZyWALL using the web configurator. The SSL protocol specifies that the SSL server (the ZyWALL) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT** > **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyWALL a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyWALL.

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyWALL's WS (web server).
2. HTTP connection requests from a web browser go to port 80 (by default) on the ZyWALL's WS (web server).

**Figure 243** HTTPS Implementation

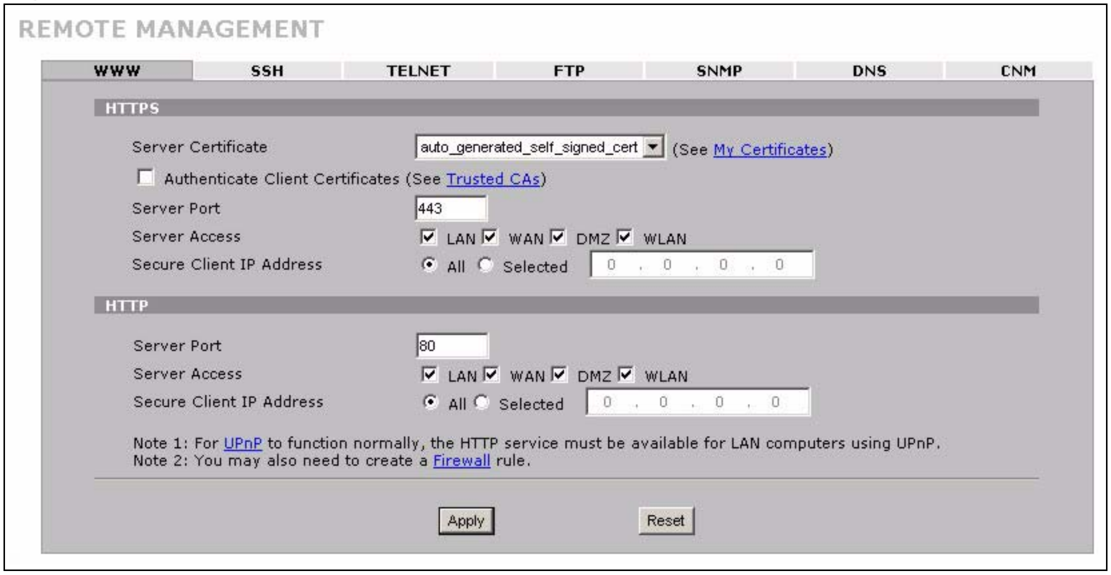


If you disable the **HTTP** service in the REMOTE MGMT WWW screen, then the ZyWALL blocks all HTTP connection attempts.

## 21.3 WWW Configuration

Click **ADVANCED** > **REMOTE MGMT** to open the **WWW** screen. Use this screen to configure the ZyWALL's HTTP and HTTPS management settings.

**Figure 244** ADVANCED > REMOTE MGMT > WWW



HTTPS

Server Certificate: auto_generated_self_signed_cert (See My Certificates)

☐ Authenticate Client Certificates (See Trusted CAs)

Server Port: 443

Server Access: ☑ LAN ☑ WAN ☑ DMZ ☑ WLAN

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

HTTP

Server Port: 80

Server Access: ☑ LAN ☑ WAN ☑ DMZ ☑ WLAN

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

Note 1: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
Note 2: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 120** ADVANCED > REMOTE MGMT > WWW

| LABEL | DESCRIPTION |
|---|---|
| HTTPS | |
| Server Certificate | Select the **Server Certificate** that the ZyWALL will use to identify itself. The ZyWALL is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL). |
| Authenticate Client Certificates | Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the ZyWALL by sending the ZyWALL a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyWALL (see Appendix E on page 657 on importing certificates for details). |
| Server Port | The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyWALL, for example 8443, then you must notify people who need to access the ZyWALL web configurator to use "https://ZyWALL IP Address:**8443**" as the URL. |
| Server Access | Select the interface(s) through which a computer may access the ZyWALL using this service.<br>You can allow only secure web configurator access by clearing all of the interface check boxes in the **HTTP Server Access** field and setting the **HTTPS Server Access** field to an interface(s). |
| Secure Client IP Address | A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| HTTP | |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 21.4 HTTPS Example

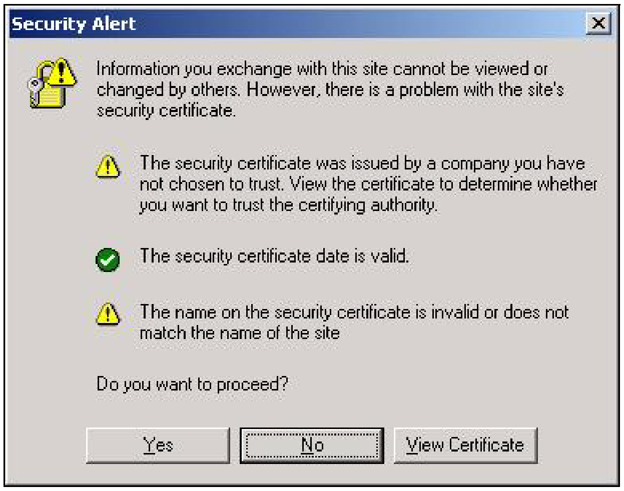
If you haven't changed the default HTTPS port on the ZyWALL, then in your browser enter "https://ZyWALL IP Address/" as the web site address where "ZyWALL IP Address" is the IP address or domain name of the ZyWALL you wish to access.

## 21.4.1 Internet Explorer Warning Messages

When you attempt to access the ZyWALL HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ZyWALL.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

**Figure 245** Security Alert Dialog Box (Internet Explorer)



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

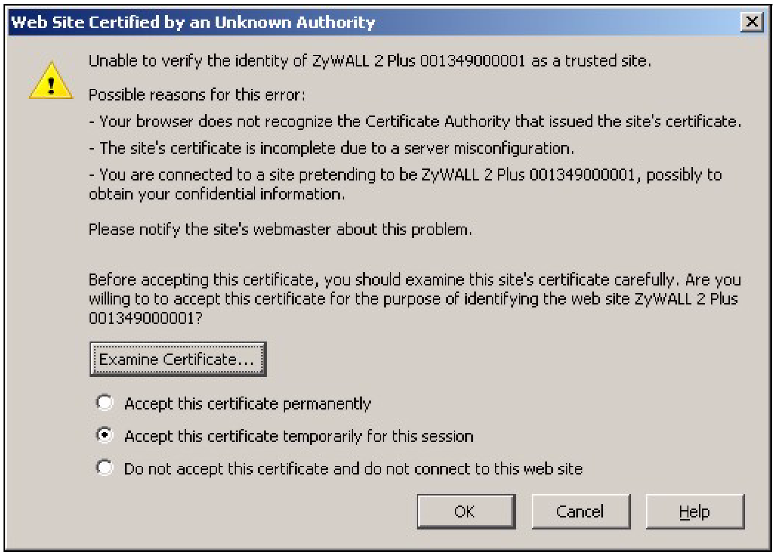
## 21.4.2 Netscape Navigator Warning Messages

When you attempt to access the ZyWALL HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the ZyWALL.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the ZyWALL's certificate into the SSL client.

**Figure 246** Security Certificate 1 (Netscape)



Unable to verify the identity of ZyWALL 2 Plus 001349000001 as a trusted site.

Possible reasons for this error:

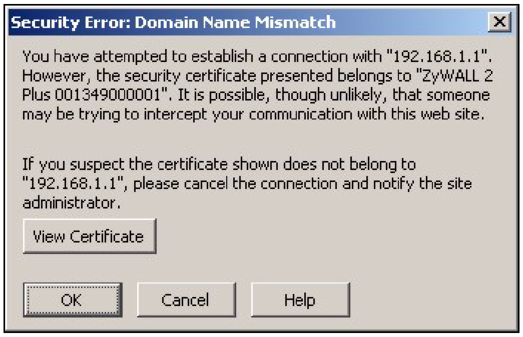
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be ZyWALL 2 Plus 001349000001, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the web site ZyWALL 2 Plus 001349000001?

○ Accept this certificate permanently
● Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this web site

**Figure 247** Security Certificate 2 (Netscape)



You have attempted to establish a connection with "192.168.1.1". However, the security certificate presented belongs to "ZyWALL 2 Plus 001349000001". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "192.168.1.1", please cancel the connection and notify the site administrator.

## 21.4.3 Avoiding the Browser Warning Messages

The following describes the main reasons that your browser displays warnings about the ZyWALL’s HTTPS server certificate and what you can do to avoid seeing the warnings.

- The issuing certificate authority of the ZyWALL’s HTTPS server certificate is not one of the browser’s trusted certificate authorities. The issuing certificate authority of the ZyWALL's factory default certificate is the ZyWALL itself since the certificate is a self-signed certificate.
  - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
  - To have the browser trust the certificates issued by a certificate authority, import the certificate authority’s certificate into your operating system as a trusted certificate. Refer to Appendix E on page 657 for details.
- The actual IP address of the HTTPS server (the IP address of the ZyWALL’s port that you are trying to access) does not match the common name specified in the ZyWALL’s HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your ZyWALL sends to HTTPS clients.
  - Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.

- Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (see Figure 250 on page 384 for an example).

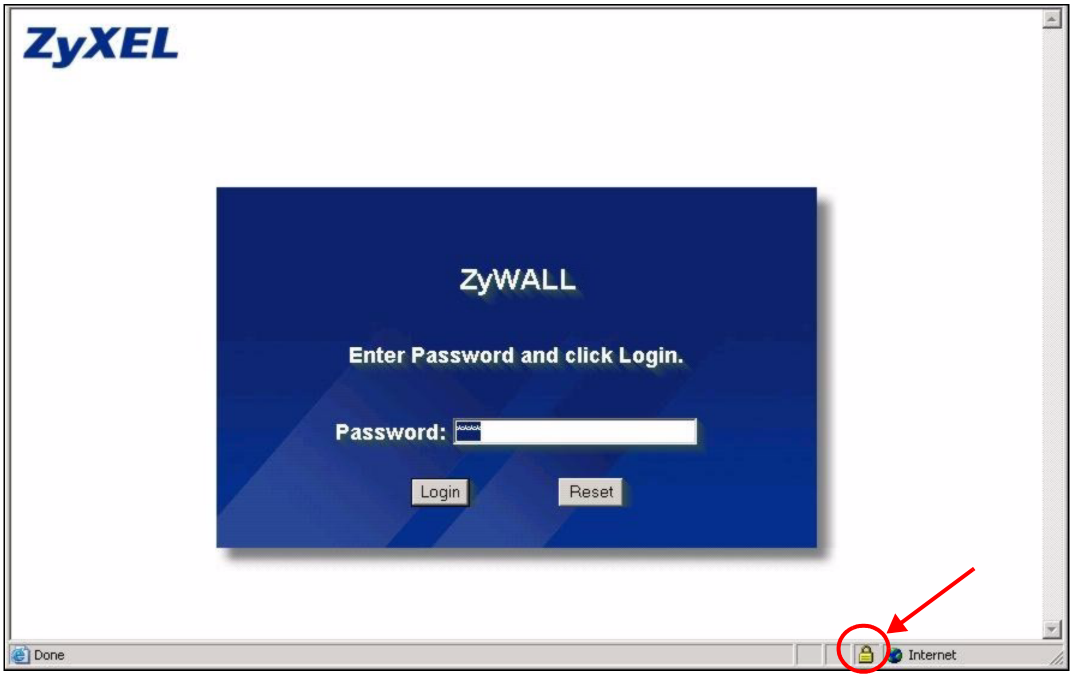
Use this procedure to have the ZyWALL use a certificate with a common name that matches the ZyWALL's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

- Create a new certificate for the ZyWALL that uses the IP address (of the ZyWALL's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.1.1, create a certificate that uses 192.168.1.1 as the common name.
- Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

## 21.4.4 Login Screen

After you accept the certificate, the ZyWALL login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

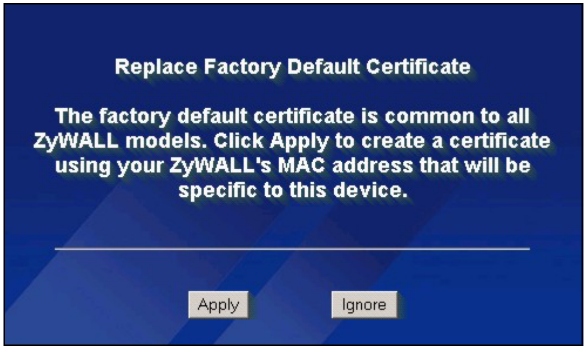
**Figure 248** Example: Lock Denoting a Secure Connection



Click **Login** and you then see the next screen.

The factory default certificate is a common default certificate for all ZyWALL models.

**Figure 249** Replace Certificate



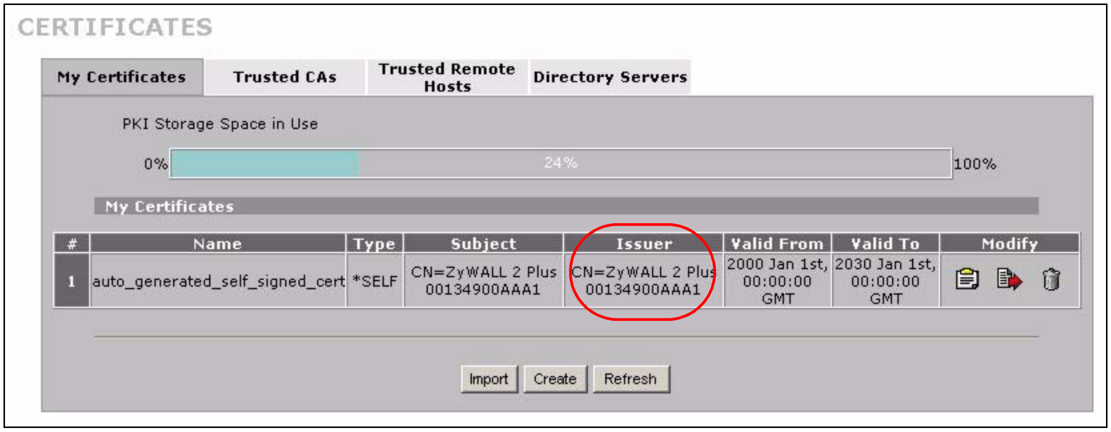
**Replace Factory Default Certificate**

**The factory default certificate is common to all ZyWALL models. Click Apply to create a certificate using your ZyWALL's MAC address that will be specific to this device.**

Apply
Ignore

Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyWALL's MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

**Figure 250** Device-specific Certificate



CERTIFICATES
My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use
0%
24%
100%

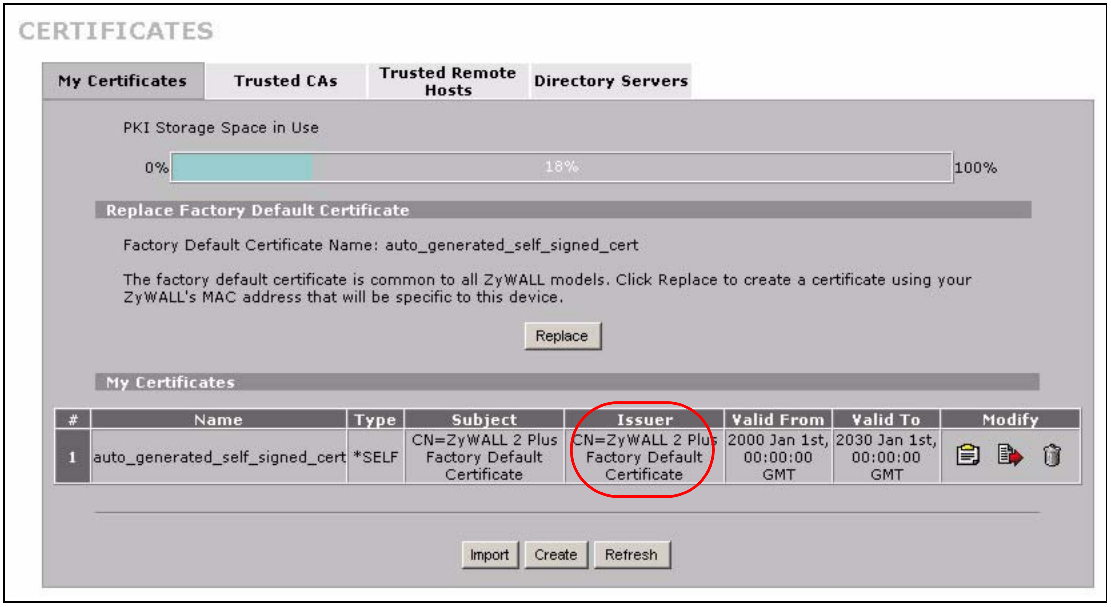
My Certificates

| # | Name | Type | Subject | Issuer | Valid From | Valid To | Modify |
|---|---|---|---|---|---|---|---|
| 1 | auto_generated_self_signed_cert | *SELF | CN=ZyWALL 2 Plus 00134900AAA1 | CN=ZyWALL 2 Plus 00134900AAA1 | 2000 Jan 1st, 00:00:00 GMT | 2030 Jan 1st, 00:00:00 GMT | |

Import
Create
Refresh

Click **Ignore** in the **Replace Certificate** screen to use the common ZyWALL certificate. You will then see this information in the **My Certificates** screen.

**Figure 251** Common ZyWALL Certificate



CERTIFICATES
My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use
0%
18%
100%

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to all ZyWALL models. Click Replace to create a certificate using your ZyWALL's MAC address that will be specific to this device.

Replace

My Certificates

| # | Name | Type | Subject | Issuer | Valid From | Valid To | Modify |
|---|---|---|---|---|---|---|---|
| 1 | auto_generated_self_signed_cert | *SELF | CN=ZyWALL 2 Plus Factory Default Certificate | CN=ZyWALL 2 Plus Factory Default Certificate | 2000 Jan 1st, 00:00:00 GMT | 2030 Jan 1st, 00:00:00 GMT | |

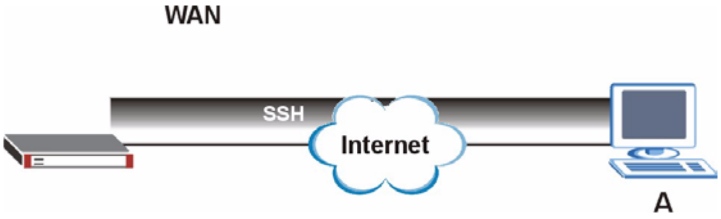
Import
Create
Refresh

## 21.5 SSH

You can use SSH (Secure SHell) to securely access the ZyWALL's SMT or command line interface. Specify which interfaces allow SSH access and from which IP address the access can come.

Unlike Telnet or FTP, which transmit data in plaintext (clear or unencrypted text), SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer **A** on the Internet uses SSH to securely connect to the WAN port of the ZyWALL for a management session.

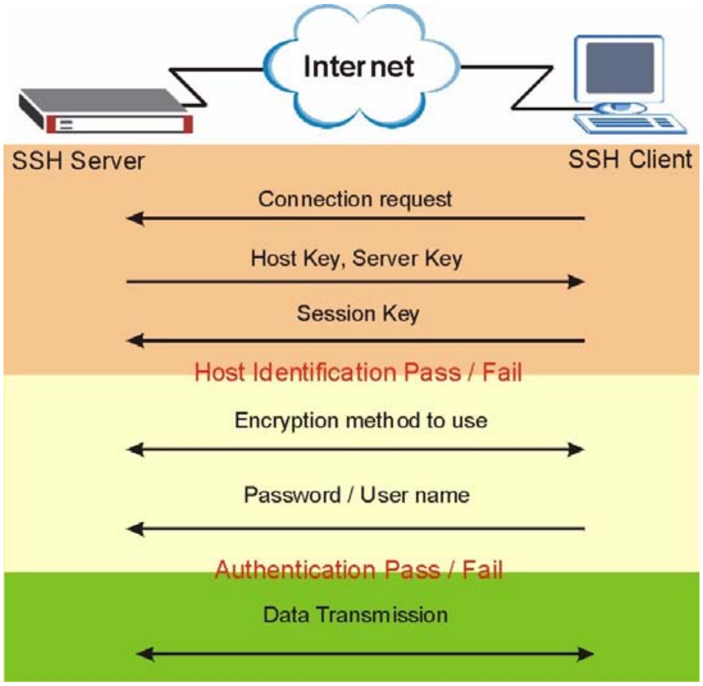
**Figure 252** SSH Communication Over the WAN Example


WAN
SSH
Internet
A

## 21.6 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

**Figure 253** How SSH Works


Internet
SSH Server
SSH Client
Connection request
Host Key, Server Key
Session Key
Host Identification Pass / Fail
Encryption method to use
Password / User name
Authentication Pass / Fail
Data Transmission

**1** Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

**2** Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

**3** Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

## 21.7 SSH Implementation on the ZyWALL

Your ZyWALL supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the ZyWALL for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

### 21.7.1 Requirements for Using SSH

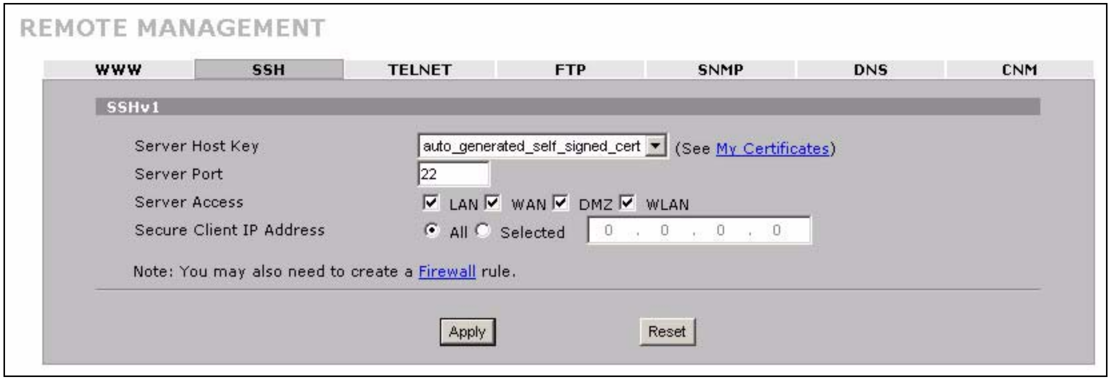
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

## 21.8 Configuring SSH

Click **ADVANCED** > **REMOTE MGMT** > **SSH** to change your ZyWALL's Secure Shell settings.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 254** ADVANCED > REMOTE MGMT > SSH



Server Host Key: auto_generated_self_signed_cert (See My Certificates)
Server Port: 22
Server Access: ☑ LAN ☑ WAN ☑ DMZ ☑ WLAN
Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 121** ADVANCED > REMOTE MGMT > SSH

| LABEL | DESCRIPTION |
|---|---|
| Server Host Key | Select the certificate whose corresponding private key is to be used to identify the ZyWALL for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 15 on page 295 for details). |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 21.9 Secure Telnet Using SSH Examples

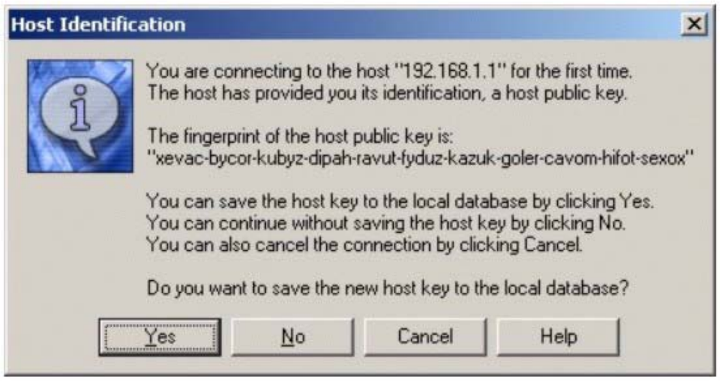
This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the ZyWALL. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

### 21.9.1 Example 1: Microsoft Windows

This section describes how to access the ZyWALL using the Secure Shell Client program.

1. Launch the SSH client and specify the connection information (IP address, port number or device name) for the ZyWALL.
2. Configure the SSH client to accept connection using SSH version 1.
3. A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

**Figure 255** SSH Example 1: Store Host Key



You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.

The fingerprint of the host public key is:
"xevac-bycor-kubyz-dipah-ravut-fyduz-kazuk-goler-cavom-hifot-sexox"

You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.

Do you want to save the new host key to the local database?

Enter the password to log in to the ZyWALL. The SMT main menu displays next.

## 21.9.2 Example 2: Linux

This section describes how to access the ZyWALL using the OpenSSH client program that comes with most Linux distributions.

1. Test whether the SSH service is available on the ZyWALL.

   Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the ZyWALL (using the default IP address of 192.168.1.1).

   A message displays indicating the SSH protocol version supported by the ZyWALL.

**Figure 256** SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2. Enter "`ssh -1 192.168.1.1`". This command forces your computer to connect to the ZyWALL using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type "`yes`" and press [ENTER].

   Then enter the password to log in to the ZyWALL.

**Figure 257** SSH Example 2: Log in

```
$ ssh –1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be 
established.
RSA1 key fingerprint is 
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of 
known hosts.
Administrator@192.168.1.1's password:
```

3 The SMT main menu displays next.

## 21.10 Secure FTP Using SSH Example

This section shows an example on file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. Refer to your SSH client program user's guide.

1 Enter "`sftp –1 192.168.1.1`". This command forces your computer to connect to the ZyWALL for secure file transfer using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type "`yes`" and press **[ENTER]**.
2 Enter the password to login to the ZyWALL.
3 Use the "`put`" command to upload a new firmware to the ZyWALL.

**Figure 258** Secure FTP: Firmware Upload Example

```
$ sftp -1 192.168.1.1
Connecting to 192.168.1.1...
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be 
established.
RSA1 key fingerprint is 
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of 
known hosts.
Administrator@192.168.1.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```

## 21.11 Telnet

You can use Telnet to access the ZyWALL's SMT or command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

## 21.12 Configuring TELNET

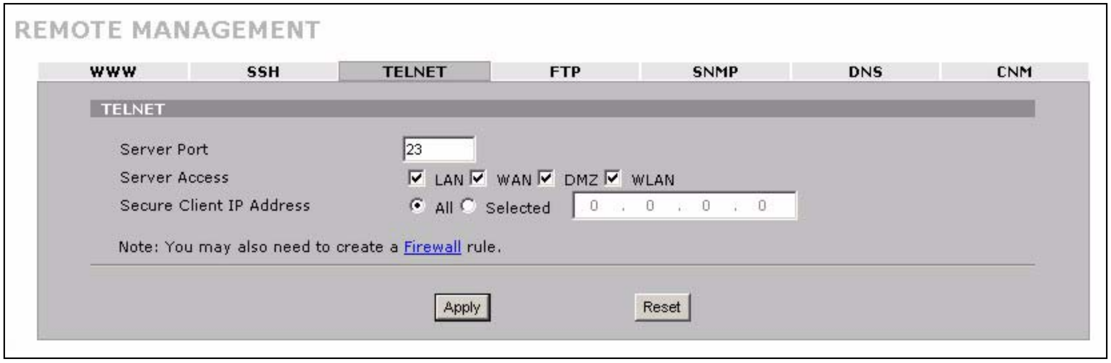
Click **ADVANCED** > **REMOTE MGMT** > **TELNET** to open the following screen. Use this screen to specify which interfaces allow Telnet access and from which IP address the access can come.

---

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

---

**Figure 259** ADVANCED > REMOTE MGMT > TELNET



Server Port: 23

Server Access: ☑ LAN ☑ WAN ☑ DMZ ☑ WLAN

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 122** ADVANCED > REMOTE MGMT > TELNET

| LABEL | DESCRIPTION |
|---|---|
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

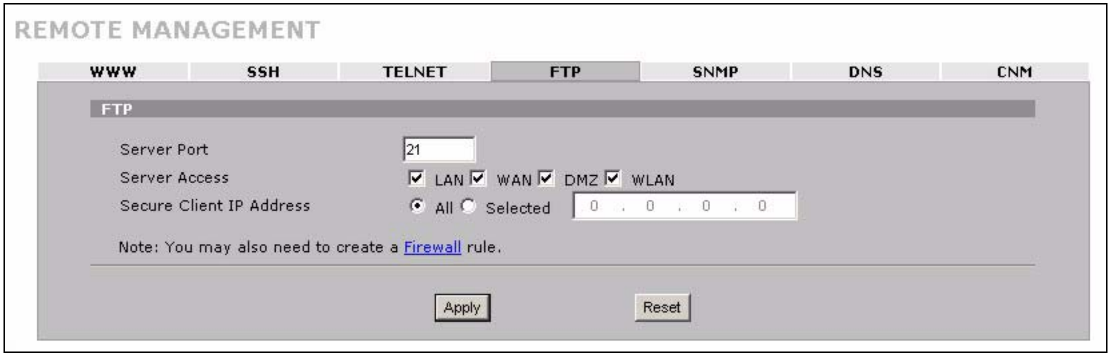
## 21.13 FTP

You can use FTP (File Transfer Protocol) to upload and download the ZyWALL's firmware and configuration files, please see the User's Guide chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyWALL's FTP settings, click **ADVANCED** > **REMOTE MGMT** > **FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 260** ADVANCED > REMOTE MGMT > FTP



Server Port: 21

Server Access: ☑ LAN ☑ WAN ☑ DMZ ☑ WLAN

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 123** ADVANCED > REMOTE MGMT > FTP

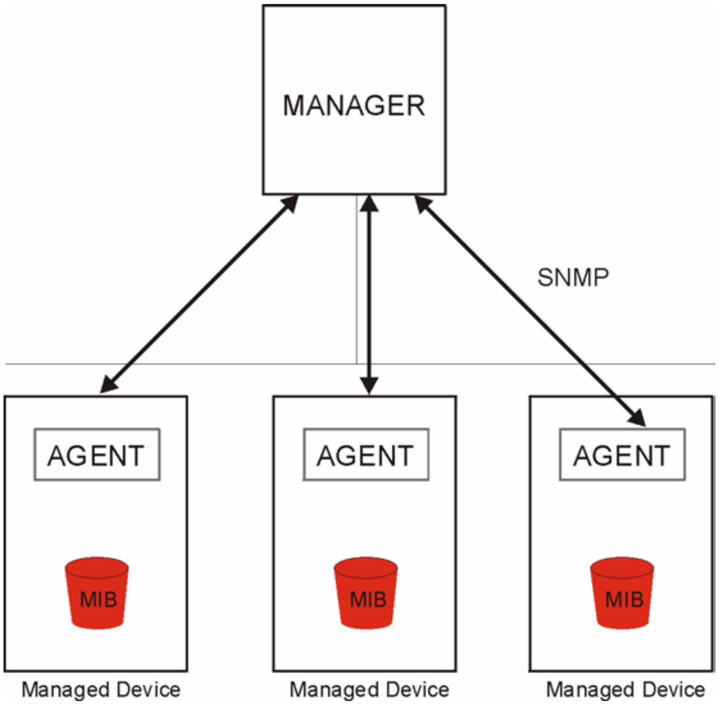
| LABEL | DESCRIPTION |
|---|---|
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 21.14 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation.

SNMP is only available if TCP/IP is configured.

**Figure 261** SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyWALL). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

### 21.14.1 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

### 21.14.2 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs:

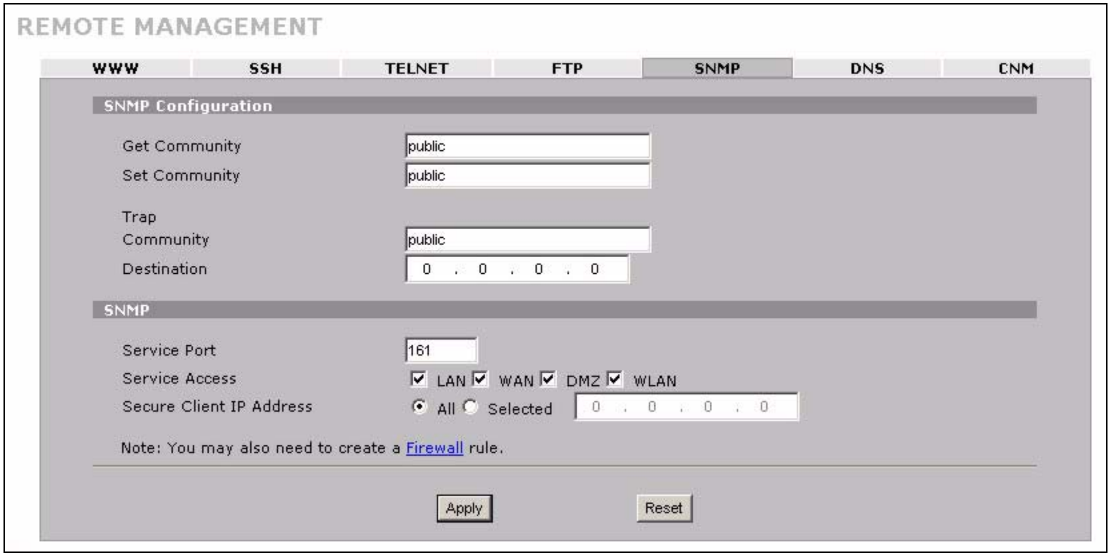
**Table 124** SNMP Traps

| TRAP # | TRAP NAME | DESCRIPTION |
|---|---|---|
| 0 | coldStart (defined in *RFC-1215*) | A trap is sent after booting (power on). |
| 1 | warmStart (defined in *RFC-1215*) | A trap is sent after booting (software reboot). |
| 4 | authenticationFailure (defined in *RFC-1215*) | A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password). |
| 6 | whyReboot (defined in ZYXEL-MIB) | A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start). |
| 6a | For intentional reboot : | A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.). |
| 6b | For fatal error : | A trap is sent with the message of the fatal code if the system reboots because of fatal errors. |

### 21.14.3 REMOTE MANAGEMENT: SNMP

To change your ZyWALL’s SNMP settings, click **ADVANCED** > **REMOTE MGMT** > **SNMP**. The screen appears as shown.

**Figure 262** ADVANCED > REMOTE MGMT > SNMP



REMOTE MANAGEMENT

SNMP Configuration

Get Community: public

Set Community: public

Trap

Community: public

Destination: 0 . 0 . 0 . 0

SNMP

Service Port: 161

Service Access: ☑ LAN ☑ WAN ☑ DMZ ☑ WLAN

Secure Client IP Address: ● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 125** ADVANCED > REMOTE MGMT > SNMP

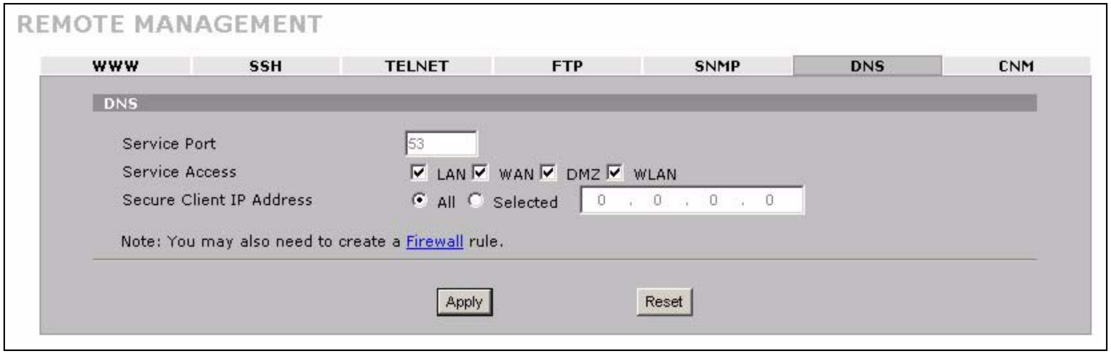
| LABEL | DESCRIPTION |
|---|---|
| SNMP Configuration | |
| Get Community | Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests. |
| Set Community | Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests. |
| Trap | |
| Community | Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests. |
| Destination | Type the IP address of the station to send your SNMP traps to. |
| SNMP | |
| Service Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Service Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 21.15 DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. Refer to Chapter 8 on page 151 for more information.

Click **ADVANCED** > **REMOTE MGMT** > **DNS** to change your ZyWALL's DNS settings. Use this screen to set from which IP address the ZyWALL will accept DNS queries and on which interface it can send them your ZyWALL's DNS settings. This feature is not available when the ZyWALL is set to bridge mode.

**Figure 263** ADVANCED > REMOTE MGMT > DNS



Service Port 53

Service Access ☑ LAN ☑ WAN ☑ DMZ ☑ WLAN

Secure Client IP Address ● All ○ Selected 0 . 0 . 0 . 0

Note: You may also need to create a Firewall rule.

The following table describes the labels in this screen.

**Table 126** ADVANCED > REMOTE MGMT > DNS

| LABEL | DESCRIPTION |
|---|---|
| Service Port | The DNS service port number is 53 and cannot be changed here. |
| Service Access | Select the interface(s) through which a computer may send DNS queries to the ZyWALL. |
| Secure Client IP Address | A secure client is a "trusted" computer that is allowed to send DNS queries to the ZyWALL.<br>Select **All** to allow any computer to send DNS queries to the ZyWALL.<br>Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the ZyWALL. |
| Apply | Click **Apply** to save your customized settings. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 21.16 Introducing Vantage CNM

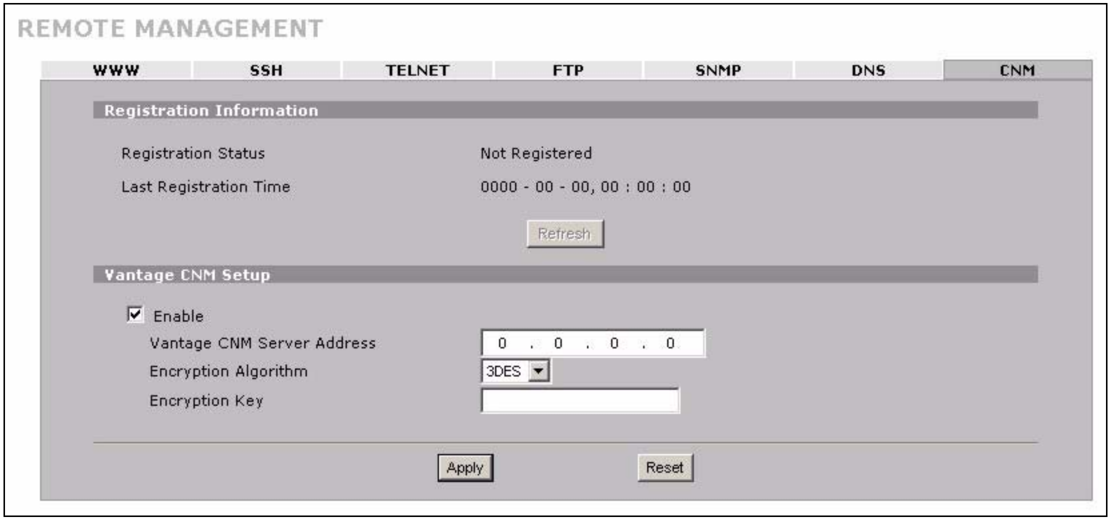
Vantage CNM (Centralized Network Management) is a browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide. See the Vantage CNM User's Guide for details.

If you allow your ZyWALL to be managed by the Vantage CNM server, then you should not configure the ZyWALL (using either the web configurator, SMT menus or commands) without notifying the Vantage CNM administrator.

## 21.17 Configuring CNM

Vantage CNM is disabled on the device by default. Click **ADVANCED** > **REMOTE MGMT** > **CNM** to configure your device's Vantage CNM settings.

**Figure 264** ADVANCED > REMOTE MGMT > CNM



Registration Status Not Registered
Last Registration Time 0000 - 00 - 00, 00 : 00 : 00

☑ Enable
Vantage CNM Server Address 0 . 0 . 0 . 0
Encryption Algorithm 3DES
Encryption Key

The following table describes the labels in this screen.

**Table 127** ADVANCED > REMOTE MGMT > CNM

| LABEL | DESCRIPTION |
|---|---|
| Registration Information | |
| Registration Status | This read only field displays **Not Registered** when **Enable** is not selected.<br>It displays **Registering** when the ZyWALL first connects with the Vantage CNM server and then **Registered** after it has been successfully registered with the Vantage CNM server. It will continue to display **Registering** until it successfully registers with the Vantage CNM server. It will not be able to register with the Vantage CNM server if:<br>The Vantage CNM server is down.<br>The Vantage CNM server IP address is incorrect.<br>The Vantage CNM server is behind a NAT router or firewall that does not forward packets through to the Vantage CNM server.<br>The encryption algorithms and/or encryption keys do not match between the ZyWALL and the Vantage CNM server. |
| Last Registration Time | This field displays the last date (year-month-date) and time (hours-minutes-seconds) that the ZyWALL registered with the Vantage CNM server. It displays all zeroes if it has not yet registered with the Vantage CNM server. |
| Refresh | Click **Refresh** to update the registration status and last registration time. |
| Vantage CNM Setup | |
| Enable | Select this check box to allow Vantage CNM to manage your ZyWALL. |
| Vantage CNM Server Address | If the Vantage server is on the same subnet as the ZyWALL, enter the private or public IP address of the Vantage server.<br>If the Vantage CNM server is on a different subnet to the ZyWALL, enter the public IP address of the Vantage server.<br>If the Vantage CNM server is on a different subnet to the ZyWALL and is behind a NAT router, enter the WAN IP address of the NAT router here. |

**Table 127** ADVANCED > REMOTE MGMT > CNM (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encryption Algorithm | The **Encryption Algorithm** field is used to encrypt communications between the ZyWALL and the Vantage CNM server. Choose from **None** (no encryption), **DES** or **3DES**. The **Encryption Key** field appears when you select **DES** or **3DES**. The ZyWALL must use the same encryption algorithm as the Vantage CNM server. |
| Encryption Key | Type eight alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the **DES** encryption algorithm and 24 alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the **3DES** encryption algorithm. The ZyWALL must use the same encryption key as the Vantage CNM server. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

### 21.17.1 Additional Configuration for Vantage CNM

If you have NAT routers or firewalls between the ZyWALL and the Vantage CNM server, you must configure them to forward TCP ports 8080 (HTTP), 443 (HTTPS) and 20 and 21 (FTP). They must also forward UDP ports 1864 and 1865.

# 22

# UPnP

This chapter introduces the Universal Plug and Play feature. This chapter is only applicable when the ZyWALL is in router mode.

## 22.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

### 22.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

### 22.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See Chapter 17 on page 331 for further information about NAT.

### 22.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyWALL allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

### 22.1.4 UPnP and ZyXEL

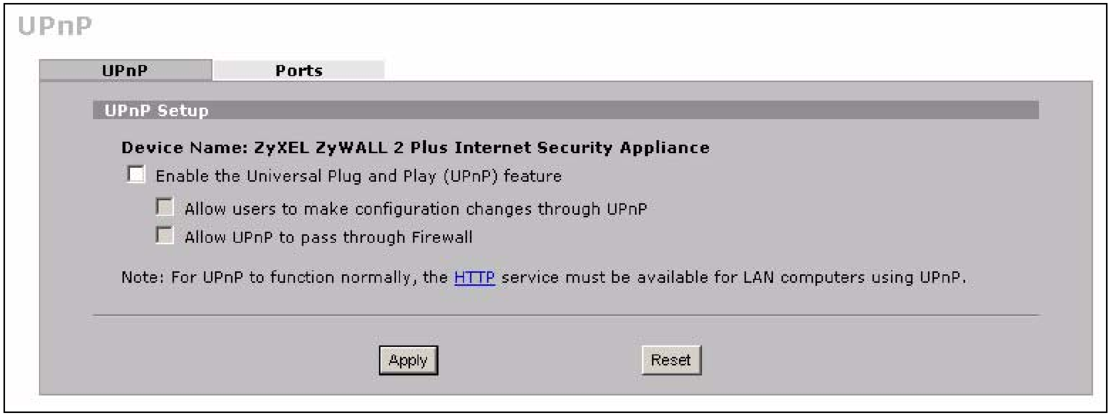
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device).

See the following sections for examples of installing and using UPnP.

## 22.2 Configuring UPnP

Click **ADVANCED** > **UPnP** to display the **UPnP** screen.

**Figure 265** ADVANCED > UPnP



Device Name: ZyXEL ZyWALL 2 Plus Internet Security Appliance

☐ Enable the Universal Plug and Play (UPnP) feature

☐ Allow users to make configuration changes through UPnP

☐ Allow UPnP to pass through Firewall

Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

The following table describes the fields in this screen.

**Table 128** ADVANCED > UPnP

| LABEL | DESCRIPTION |
|---|---|
| UPnP Setup | |
| Device Name | This identifies the ZyXEL device in UPnP applications. |
| Enable the Universal Plug and Play (UPnP) feature | Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyWALL's IP address (although you must still enter the password to access the web configurator). |
| Allow users to make configuration changes through UPnP | Select this check box to allow UPnP-enabled applications to automatically configure the ZyWALL so that they can communicate through the ZyWALL, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. |
| Allow UPnP to pass through Firewall | Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall.<br>Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets). |

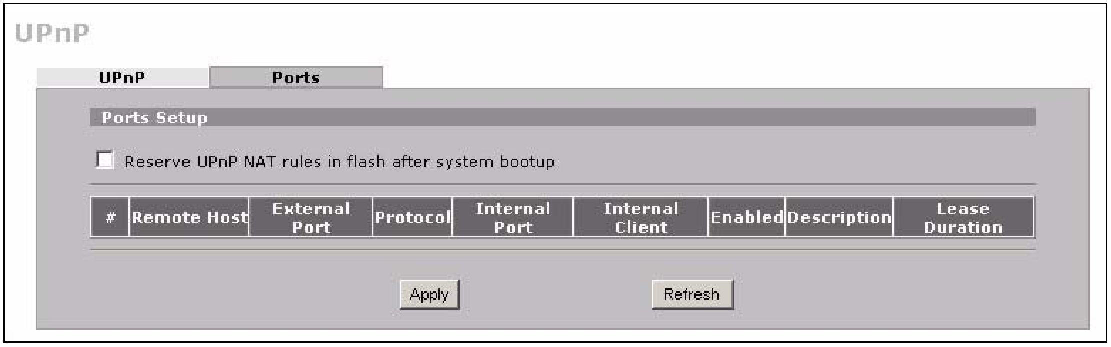
**Table 128** ADVANCED > UPnP

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 22.3 Displaying UPnP Port Mapping

Click **ADVANCED** > **UPnP** > **Ports** to display the **UPnP Ports** screen. Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL.

**Figure 266** ADVANCED > UPnP > Ports



The following table describes the labels in this screen.

**Table 129** ADVANCED > UPnP > Ports

| LABEL | DESCRIPTION |
|---|---|
| Reserve UPnP NAT rules in flash after system bootup | Select this check box to have the ZyWALL retain UPnP created NAT rules even after restarting. If you use UPnP and you set a port on your computer to be fixed for a specific service (for example FTP for file transfers), this option allows the ZyWALL to keep a record when your computer uses UPnP to create a NAT forwarding rule for that service. |
| The following read-only table displays information about the UPnP-created NAT mapping rule entries in the ZyWALL's NAT routing table. | |
| # | This is the index number of the UPnP-created NAT mapping rule entry. |
| Remote Host | This field displays the source IP address (on the WAN) of inbound IP packets. Since this is often a wildcard, the field may be blank. When the field is blank, the ZyWALL forwards all traffic sent to the **External Port** on the WAN interface to the **Internal Client** on the **Internal Port**. When this field displays an external IP address, the NAT rule has the ZyWALL forward inbound packets to the **Internal Client** from that IP address only. |
| External Port | This field displays the port number that the ZyWALL "listens" on (on the WAN port) for connection requests destined for the NAT rule's **Internal Port** and **Internal Client**. The ZyWALL forwards incoming packets (from the WAN) with this port number to the **Internal Client** on the **Internal Port** (on the LAN). If the field displays "0", the ZyWALL ignores the **Internal Port** value and forwards requests on all external port numbers (that are otherwise unmapped) to the **Internal Client**. |
| Protocol | This field displays the protocol of the NAT mapping rule (TCP or UDP). |
| Internal Port | This field displays the port number on the **Internal Client** to which the ZyWALL should forward incoming connection requests. |

**Table 129** ADVANCED > UPnP > Ports (continued)

| LABEL | DESCRIPTION |
|---|---|
| Internal Client | This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings. |
| Enabled | This field displays whether or not this UPnP-created NAT mapping rule is turned on. The UPnP-enabled device that connected to the ZyWALL and configured the UPnP-created NAT mapping rule on the ZyWALL determines whether or not the rule is enabled. |
| Description | This field displays a text explanation of the NAT mapping rule. |
| Lease Duration | This field displays a dynamic port-mapping rule’s time to live (in seconds). It displays “0” if the port mapping is static. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Refresh | Click **Refresh** update the screen’s table. |

## 22.4 Installing UPnP in Windows Example

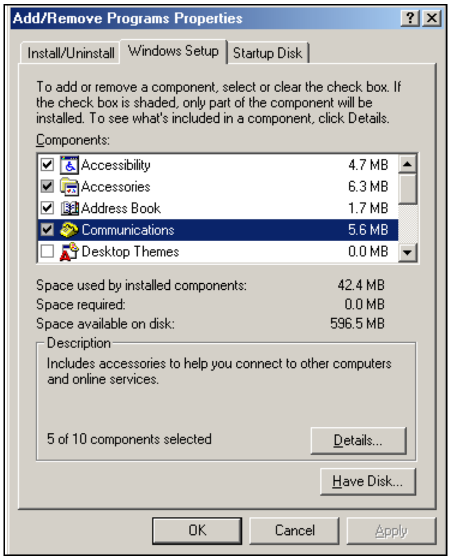
This section shows how to install UPnP in Windows Me and Windows XP.

### 22.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

1 Click **Start**, **Settings** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
Components:
Description
Details...
Have Disk...
OK
Cancel
Apply

To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

| | | |
|---|---|---|
| ☑ | Accessibility | 4.7 MB |
| ☑ | Accessories | 6.3 MB |
| ☑ | Address Book | 1.7 MB |
| ☑ | Communications | 5.6 MB |
| ☐ | Desktop Themes | 0.0 MB |

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 596.5 MB

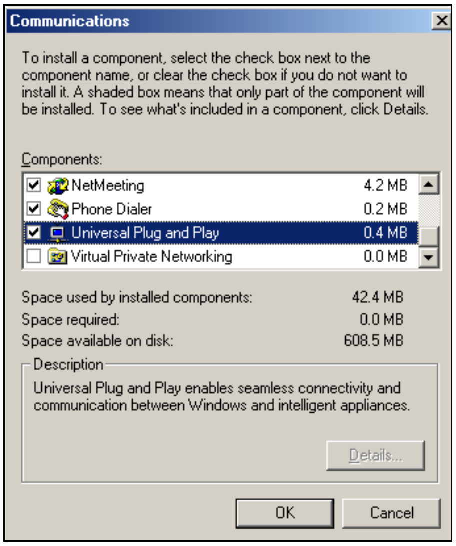
Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

4 Click **OK** to go back to the **Add/ Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.


Communications
Components:
Description
Details...
OK
Cancel

To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

| | | |
|---|---|---|
| ☑ | NetMeeting | 4.2 MB |
| ☑ | Phone Dialer | 0.2 MB |
| ☑ | Universal Plug and Play | 0.4 MB |
| ☐ | Virtual Private Networking | 0.0 MB |

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 608.5 MB

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

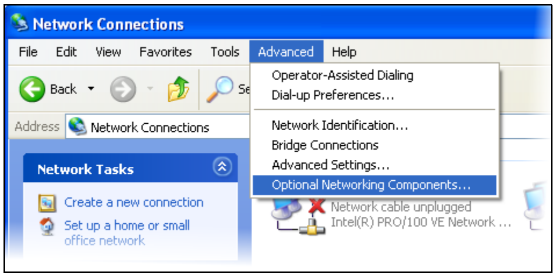
## 22.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

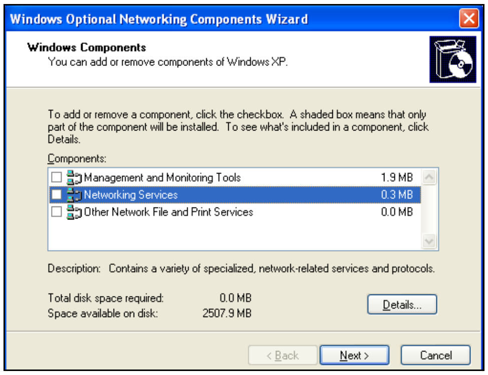
1 Click **Start**, **Settings** and **Control Panel**.

2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**
The **Windows Optional Networking Components Wizard** window displays.


Network Connections
File Edit View Favorites Tools Advanced Help
Back
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Operator-Assisted Dialing
Dial-up Preferences…
Network Identification…
Bridge Connections
Advanced Settings…
Optional Networking Components…
Network cable unplugged
Intel(R) PRO/100 VE Network …

4 Select **Networking Service** in the **Components** selection box and click **Details**.


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

| | | |
|---|---|---|
| ☐ | Management and Monitoring Tools | 1.9 MB |
| ☐ | Networking Services | 0.3 MB |
| ☐ | Other Network File and Print Services | 0.0 MB |

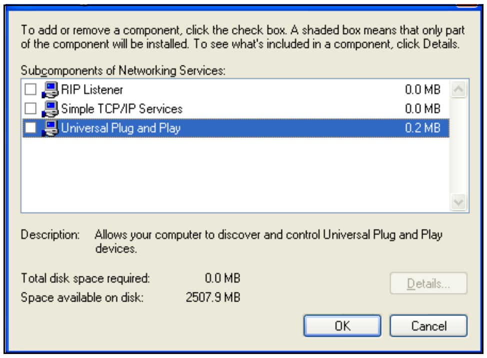
Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 2507.9 MB

Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.


To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

| | | |
|---|---|---|
| ☐ | RIP Listener | 0.0 MB |
| ☐ | Simple TCP/IP Services | 0.0 MB |
| ☐ | Universal Plug and Play | 0.2 MB |

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB
Space available on disk: 2507.9 MB

Details...
OK
Cancel

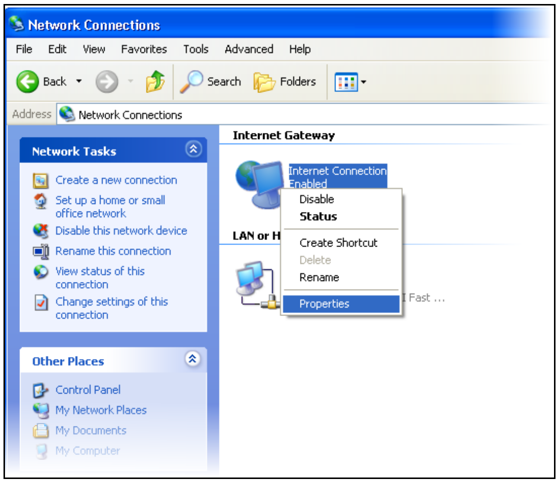
## 22.5 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

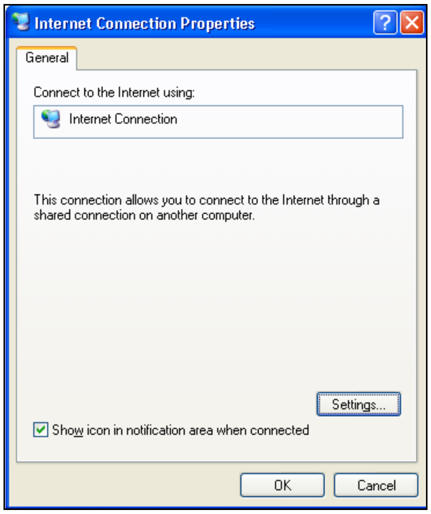
Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

### 22.5.1 Auto-discover Your UPnP-enabled Network Device

1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under **Internet Gateway**.
2. Right-click the icon and select **Properties**.


Network Connections
File Edit View Favorites Tools Advanced Help
Back
Search
Folders
Address
Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Rename this connection
View status of this connection
Change settings of this connection
Other Places
Control Panel
My Network Places
My Documents
My Computer
Internet Gateway
Internet Connection Enabled
LAN or H
Disable
Status
Create Shortcut
Delete
Rename
Properties
Fast ...

3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.


Internet Connection Properties
General
Settings...
OK
Cancel

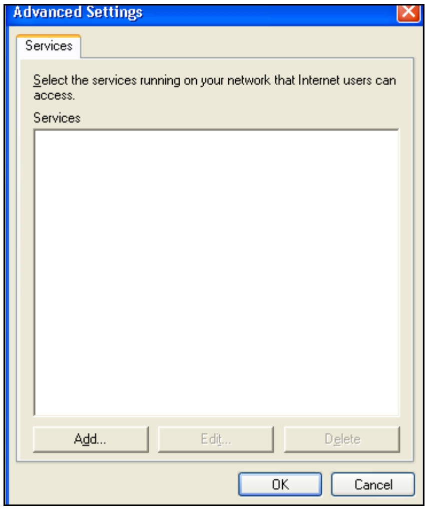
Connect to the Internet using:

Internet Connection

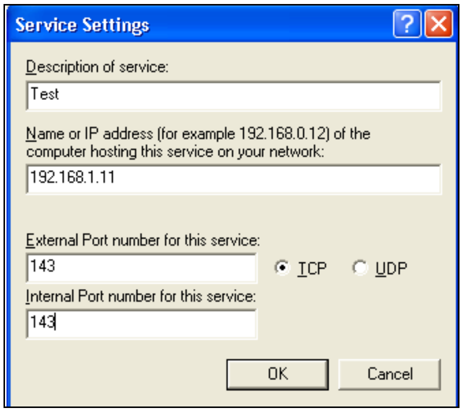
This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

You may edit or delete the port mappings or click **Add** to manually add port mappings.


Advanced Settings
Services
Services
Add...
Edit...
Delete
OK
Cancel

Select the services running on your network that Internet users can access.



Service Settings
OK
Cancel

Description of service: Test

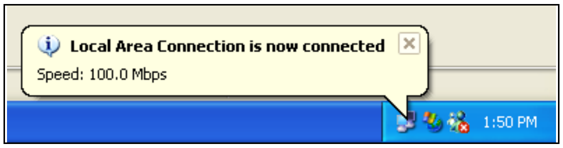
Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network: 192.168.1.11

External Port number for this service: 143 ● TCP ○ UDP

Internal Port number for this service: 143

When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

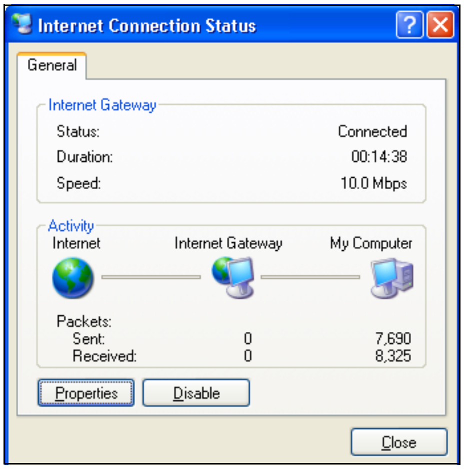
4 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.



Local Area Connection is now connected

Speed: 100.0 Mbps

5 Double-click the icon to display your current Internet connection status.



Internet Connection Status
General
Internet Gateway
Activity
Internet
Internet Gateway
My Computer
Properties
Disable
Close

Status: Connected

Duration: 00:14:38

Speed: 10.0 Mbps

| Packets: | Internet Gateway | My Computer |
|---|---|---|
| Sent: | 0 | 7,690 |
| Received: | 0 | 8,325 |

## 22.5.2 Web Configurator Easy Access

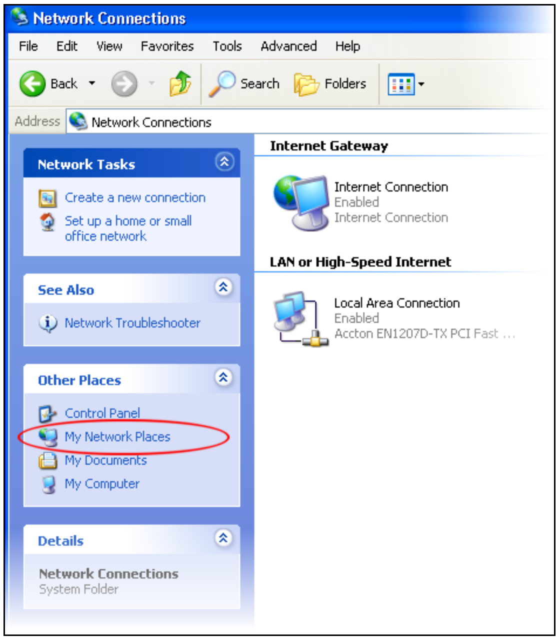
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

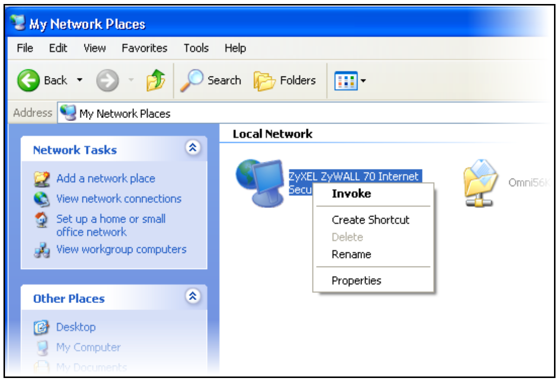
2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

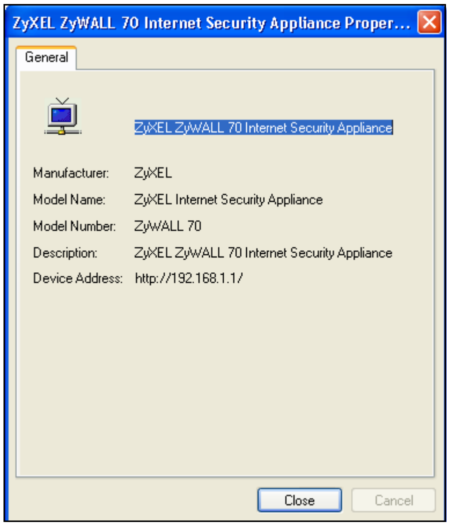

Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
See Also
Network Troubleshooter
Other Places
Control Panel
My Network Places
My Documents
My Computer
Details
Network Connections
System Folder
Internet Gateway
Internet Connection
Enabled
Internet Connection
LAN or High-Speed Internet
Local Area Connection
Enabled
Accton EN1207D-TX PCI Fast …

4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.


My Network Places
File Edit View Favorites Tools Help
Back Search Folders
Address My Network Places
Network Tasks
Add a network place
View network connections
Set up a home or small office network
View workgroup computers
Other Places
Desktop
My Computer
My Documents
Local Network
ZyXEL ZyWALL 70 Internet Secu
Invoke
Create Shortcut
Delete
Rename
Properties
Omni56

**6** Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.


ZyXEL ZyWALL 70 Internet Security Appliance Proper...
General
Close
Cancel

ZyXEL ZyWALL 70 Internet Security Appliance

Manufacturer: ZyXEL
Model Name: ZyXEL Internet Security Appliance
Model Number: ZyWALL 70
Description: ZyXEL ZyWALL 70 Internet Security Appliance
Device Address: http://192.168.1.1/

# 23

# Custom Application

This chapter covers how to set the ZyWALL's to monitor custom port numbers for specific applications.

## 23.1 Custom Applicaton

Use custom application to have the ZyWALL's ALG and content filtering features monitor traffic on custom ports, in addition to the default ports.

By default, these ZyWALL features monitor traffic for the following protocols on these port numbers.

- FTP: 21
- SIP: 5060
- H.323: 1720
- SMTP: 25
- POP3: 110
- HTTP: 80

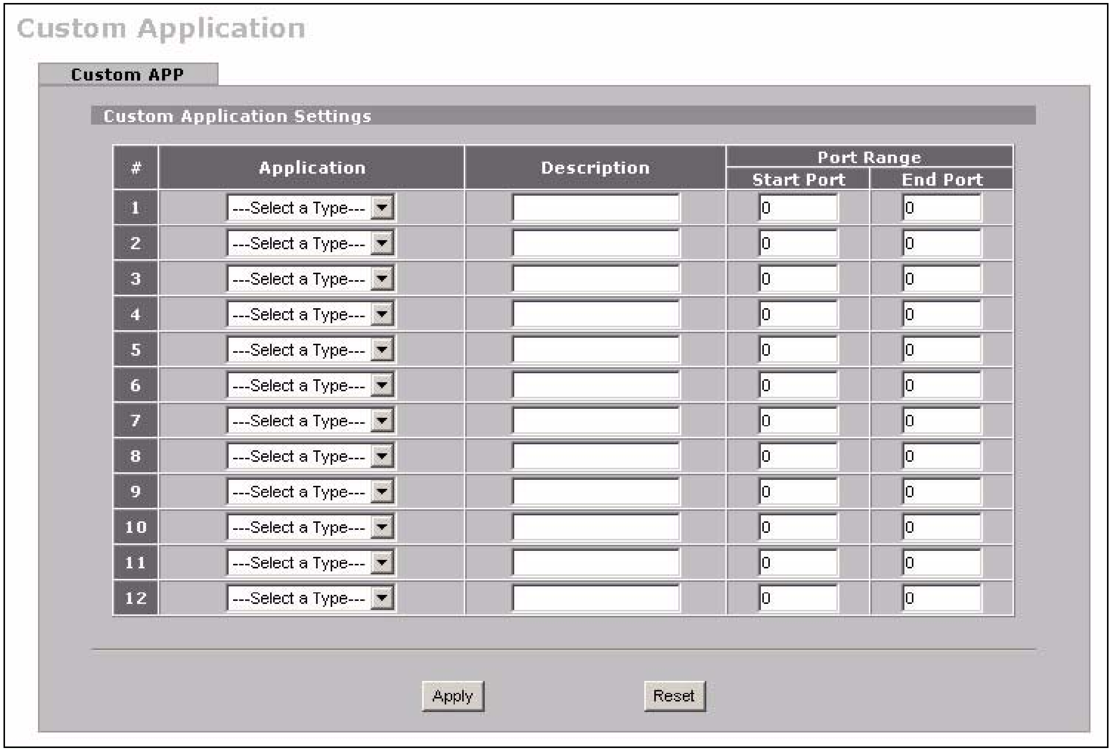
Changes in the **Custom APP** screen do not apply to the firewall.

## 23.2 Custom Applicaton Configuration

Click **ADVANCED** > **Custom APP** to open the **Custom Application** screen.

This screen only specifies what port numbers the ZyWALL checks for specific protocol traffic. Use other screens to enable or disable the monitoring of the protocol traffic.

**Figure 267** ADVANCED > Custom APP



| # | Application | Description | Port Range |  |
|---|---|---|---|---|
|  |  |  | Start Port | End Port |
| 1 | ---Select a Type--- |  | 0 | 0 |
| 2 | ---Select a Type--- |  | 0 | 0 |
| 3 | ---Select a Type--- |  | 0 | 0 |
| 4 | ---Select a Type--- |  | 0 | 0 |
| 5 | ---Select a Type--- |  | 0 | 0 |
| 6 | ---Select a Type--- |  | 0 | 0 |
| 7 | ---Select a Type--- |  | 0 | 0 |
| 8 | ---Select a Type--- |  | 0 | 0 |
| 9 | ---Select a Type--- |  | 0 | 0 |
| 10 | ---Select a Type--- |  | 0 | 0 |
| 11 | ---Select a Type--- |  | 0 | 0 |
| 12 | ---Select a Type--- |  | 0 | 0 |

The following table describes the labels in this screen.

**Table 130** ADVANCED > Custom APP

| LABEL | DESCRIPTION |
|---|---|
| Application | Select the application for which you want the ZyWALL to monitor specific ports. You can use the same application in more than one entry. To remove an entry, select **Select a Type**. |
| Description | Enter information about the reason for monitoring custom port numbers for this protocol. |
| Start Port | Enter the starting port for the range that the ZyWALL is to monitor for this application. If you are only entering a single port number, enter it here. |
| End Port | Enter the ending port for the range that the ZyWALL is to monitor for this application. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 24

# ALG Screen

This chapter covers how to use the ZyWALL's ALG feature to allow certain applications to pass through the ZyWALL.

## 24.1 ALG Introduction

An Application Layer Gateway (ALG) manages a specific protocol (such as SIP, H.323 or FTP) at the application layer. The ZyWALL can function as an ALG to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyWALL.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ZyWALL examines and uses IP address and port number information embedded in the data stream. When a device behind the ZyWALL uses an application for which the ZyWALL has ALG service enabled, the ZyWALL translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and dynamically creates implicit NAT port forwarding and firewall rules for the application's traffic to come in from the WAN to the LAN.

### 24.1.1 ALG and NAT

The ZyWALL dynamically creates an implicit NAT session for the application's traffic from the WAN to the LAN.

The ALG on the ZyWALL supports all NAT mapping types, including **One to One**, **Many to One**, **Many to Many Overload** and **Many One to One**.

### 24.1.2 ALG and the Firewall

The ZyWALL uses the dynamic port that the session uses for data transfer in creating an implicit temporary firewall rule for the session's traffic. The firewall rule only allows the session's traffic to go through in the direction that the ZyWALL determines from its inspection of the data payload of the application's packets. The firewall rule is automatically deleted after the application's traffic has gone through.

## 24.2 FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. The FTP ALG allows TCP packets with a port 21 destination to pass through. If the FTP server is located on the LAN, you must also configure NAT port forwarding and firewall rules if you want to allow access to the server from the WAN.

## 24.3 H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

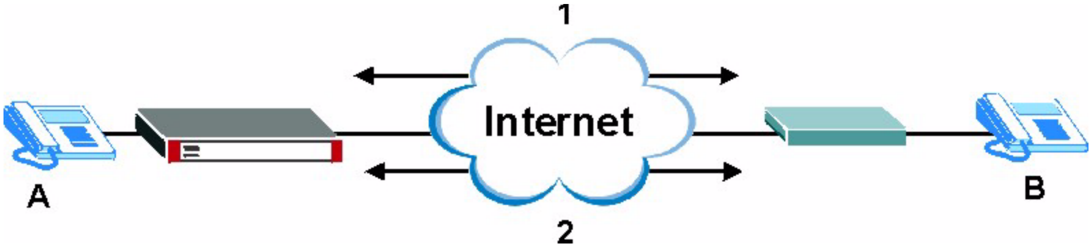
## 24.4 RTP

When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

### 24.4.1 H.323 ALG Details

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the ZyWALL routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- You must configure the firewall and port forwarding to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ or WLAN). The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

**Figure 268** H.323 ALG Example



- The H.323 ALG operates on TCP packets with a port 1720 destination.
- The ZyWALL allows H.323 audio connections.

- The ZyWALL can also apply bandwidth management to traffic that goes through the H.323 ALG.

## 24.5 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

### 24.5.1 STUN

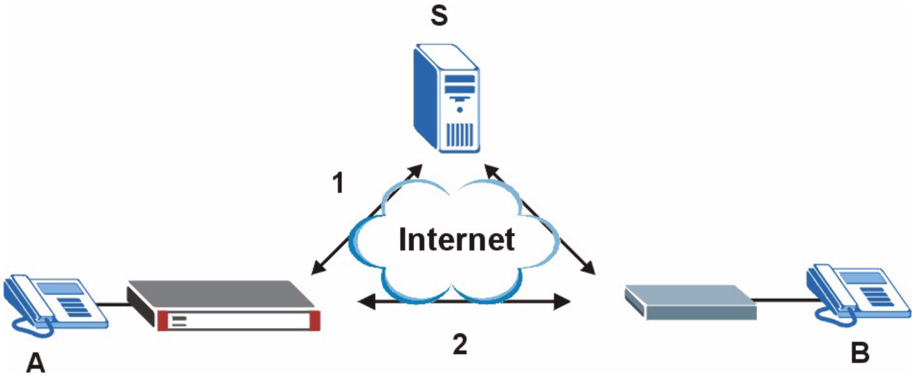
STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the VoIP device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the VoIP device to find the public IP address that NAT assigned, so the VoIP device can embed it in the SIP data stream. See RFC 3489 for details on STUN. You do not need to use STUN for devices behind the ZyWALL if you enable the SIP ALG.

### 24.5.2 SIP ALG Details

- SIP clients can be connected to the LAN, WLAN or DMZ. A SIP server must be on the WAN.
- You can make and receive calls between the LAN and the WAN, between the WLAN and the WAN and/or between the DMZ and the WAN. You cannot make a call between the LAN and the LAN, between the LAN and the DMZ, between the LAN and the WLAN, between the DMZ and the DMZ, and so on.
- The SIP ALG allows UDP packets with a port 5060 destination to pass through.
- The ZyWALL allows SIP audio connections.

The following example shows SIP signaling (1) and audio (2) sessions between SIP clients A and B and the SIP server (S).

**Figure 269** SIP ALG Example



### 24.5.3 SIP Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL.

If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout default (60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period.

### 24.5.4 SIP Audio Session Timeout

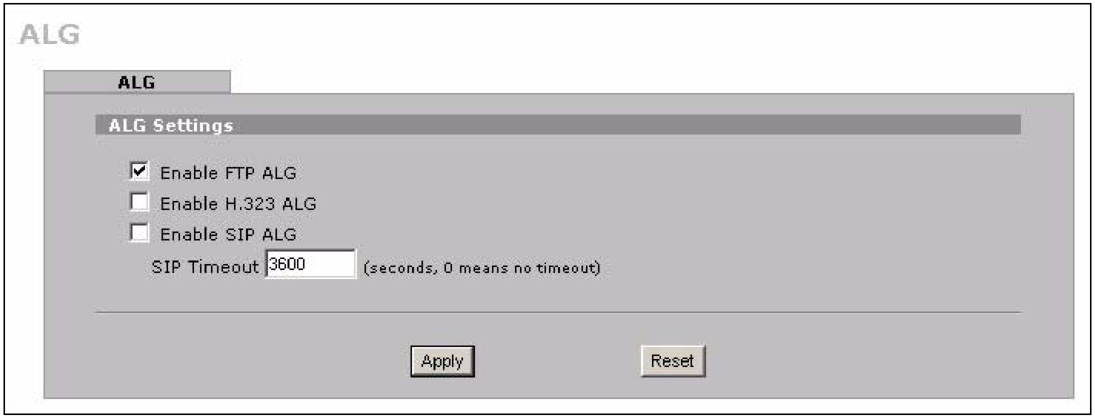
If no voice packets go through the SIP ALG before the timeout period (default 5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

## 24.6 ALG Screen

Click **ADVANCED** > **ALG** to open the **ALG** screen. Use the **ALG** screen to turn individual ALGs off or on and set the SIP timeout.

If the ZyWALL provides an ALG for a service, you must enable the ALG in order to perform bandwidth management on that service’s traffic.

**Figure 270** ADVANCED > ALG



☑ Enable FTP ALG
☐ Enable H.323 ALG
☐ Enable SIP ALG
SIP Timeout 3600 (seconds, 0 means no timeout)

The following table describes the labels in this screen.

**Table 131** ADVANCED > ALG

| LABEL | DESCRIPTION |
|---|---|
| Enable FTP ALG | Select this check box to allow FTP sessions to pass through the ZyWALL. FTP (File Transfer Program) is a program that enables fast transfer of files, including large files that may not be possible by e-mail. |
| Enable H.323 ALG | Select this check box to allow H.323 sessions to pass through the ZyWALL. H.323 is a protocol used for audio communications over networks. |
| Enable SIP ALG | Select this check box to allow SIP sessions to pass through the ZyWALL. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol. |
| SIP Timeout | Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL.<br>If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout (default 60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period. Enter the SIP signaling session timeout value. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# PART V

# Logs and Maintenance

Logs Screens (419)
Maintenance (447)

# 25

# Logs Screens

This chapter contains information about configuring general log settings and viewing the ZyWALL's logs. Refer to Section 25.5 on page 430 for example log message explanations.

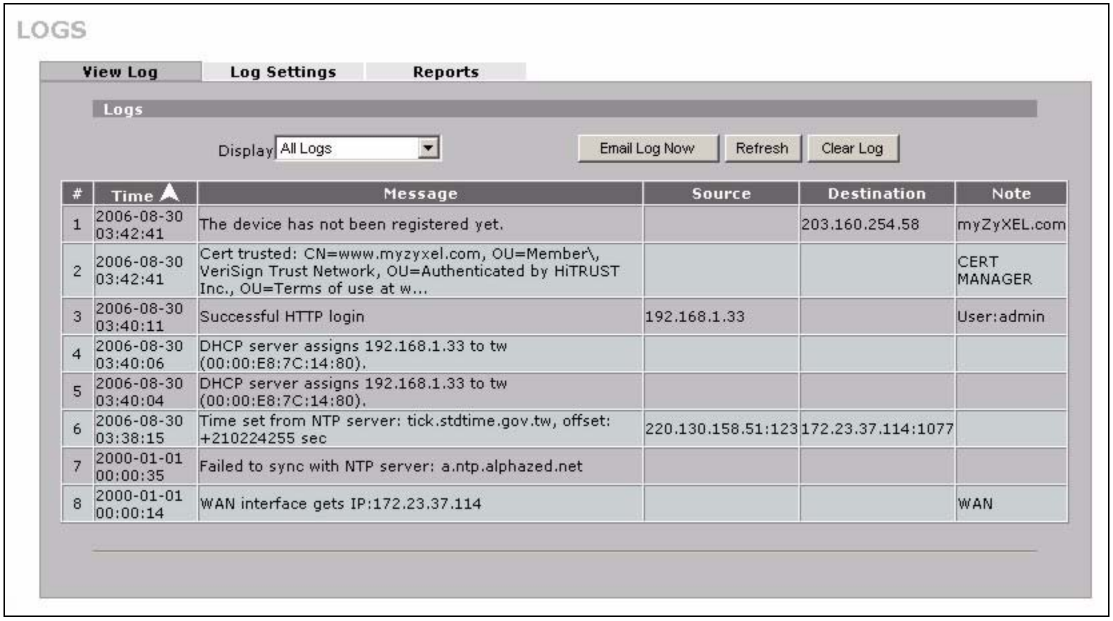
## 25.1 Configuring View Log

The web configurator allows you to look at all of the ZyWALL's logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 25.3 on page 422). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

**Figure 271** LOGS > View Log



| # | Time ▲ | Message | Source | Destination | Note |
|---|---|---|---|---|---|
| 1 | 2006-08-30 03:42:41 | The device has not been registered yet. | | 203.160.254.58 | myZyXEL.com |
| 2 | 2006-08-30 03:42:41 | Cert trusted: CN=www.myzyxel.com, OU=Member\, VeriSign Trust Network, OU=Authenticated by HiTRUST Inc., OU=Terms of use at w... | | | CERT MANAGER |
| 3 | 2006-08-30 03:40:11 | Successful HTTP login | 192.168.1.33 | | User:admin |
| 4 | 2006-08-30 03:40:06 | DHCP server assigns 192.168.1.33 to tw (00:00:E8:7C:14:80). | | | |
| 5 | 2006-08-30 03:40:04 | DHCP server assigns 192.168.1.33 to tw (00:00:E8:7C:14:80). | | | |
| 6 | 2006-08-30 03:38:15 | Time set from NTP server: tick.stdtime.gov.tw, offset: +210224255 sec | 220.130.158.51:123 | 172.23.37.114:1077 | |
| 7 | 2000-01-01 00:00:35 | Failed to sync with NTP server: a.ntp.alphazed.net | | | |
| 8 | 2000-01-01 00:00:14 | WAN interface gets IP:172.23.37.114 | | | WAN |

The following table describes the labels in this screen.

**Table 132** LOGS > View Log

| LABEL | DESCRIPTION |
|---|---|
| Display | The categories that you select in the **Log Settings** page (see Section 25.3 on page 422) display in the drop-down list box.<br>Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page. |
| # | This field displays the log number. |
| Time | This field displays the time the log was recorded. See Section 26.4 on page 449 to configure the ZyWALL's time and date. |
| Message | This field states the reason for the log. |
| Source | This field lists the source IP address and the port number of the incoming packet. |
| Destination | This field lists the destination IP address and the port number of the incoming packet. |
| Note | This field displays additional information about the log entry. |
| Email Log Now | Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**, see Section 25.3 on page 422). |
| Refresh | Click **Refresh** to renew the log screen. |
| Clear Log | Click **Clear Log** to delete all the logs. |

## 25.2 Log Description Example

The following is an example of how a log displays in the command line interpreter and a description of the sample log. Refer to the appendices for more log message descriptions and details on using the command line interpreter to display logs.

```
#   .time                   source                  destination
notes

    message

  5|06/08/2004 05:58:20 |172.16.4.187:137      |172.16.255.255:137
|ACCESS BLOCK

    Firewall default policy: UDP (W to W/ZW)
```

**Table 133** Log Description Example

| LABEL | DESCRIPTION |
|---|---|
| # | This is log number five. |
| time | The log was generated on June 8, 2004 at 5:58 and 20 seconds AM. |
| source | The log was generated due to a NetBIOS packet sent from IP address 172.16.4.187 port 137. |
| destination | The NetBIOS packet was sent to the 172.16.255.255 subnet port 137. This was a NetBIOS UDP broadcast packet meant to discover devices on the network. |

**Table 133** Log Description Example

| LABEL | DESCRIPTION |
|---|---|
| notes | The ZyWALL blocked the packet. |
| message | The ZyWALL blocked the packet in accordance with the firewall’s default policy of blocking sessions that are initiated from the WAN. “UDP” means that this was a User Datagram Protocol packet. “W to W/ZW” indicates that the packet was traveling from the WAN to the WAN or the ZyWALL. |

## 25.2.1 About the Certificate Not Trusted Log

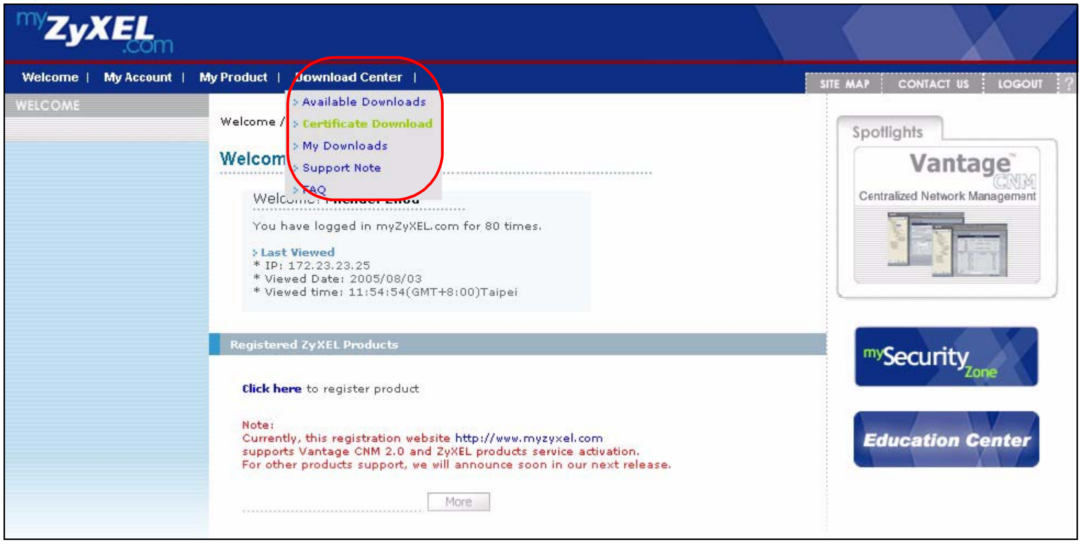
myZyXEL.com and the update server use certificates signed by VeriSign to identify themselves. If the ZyWALL does not have a CA certificate signed by VeriSign as a trusted CA, the ZyWALL will not trust the certificate from myZyXEL.com and the update server. The ZyWALL will generate a log like "Due to error code(11), cert not trusted: SSL/TLS peer certif..." for every time it attempt to establish a (HTTPS) connection with myZyXEL.com and the update server. The V4.00 default configuration file includes a trusted CA certificate signed by VeriSign. If you upgraded to ZyNOS V4.00 firmware without uploading the V4.00 default configuration file, you can download a CA certificate signed by VeriSign from myZyXEL.com and import it into the ZyWALL as a trusted CA. This will stop the ZyWALL from generating this log every time it attempts to connect with myzyxel.com and the update server.

Follow the steps below to download the certificate from myZyXEL.com.

1 Go to http://www.myZyXEL.com and log in with your account.

2 Click **Download Center** and then **Certificate Download**.

**Figure 272** myZyXEL.com: Download Center



myZyXEL.com
Welcome | My Account | My Product | Download Center |
Available Downloads
Certificate Download
My Downloads
Support Note
FAQ
SITE MAP
CONTACT US
LOGOUT
WELCOME
Welcome /
Welcom
Spotlights
Vantage CNM
Centralized Network Management
mySecurity Zone
Education Center
Registered ZyXEL Products
More

You have logged in myZyXEL.com for 80 times.

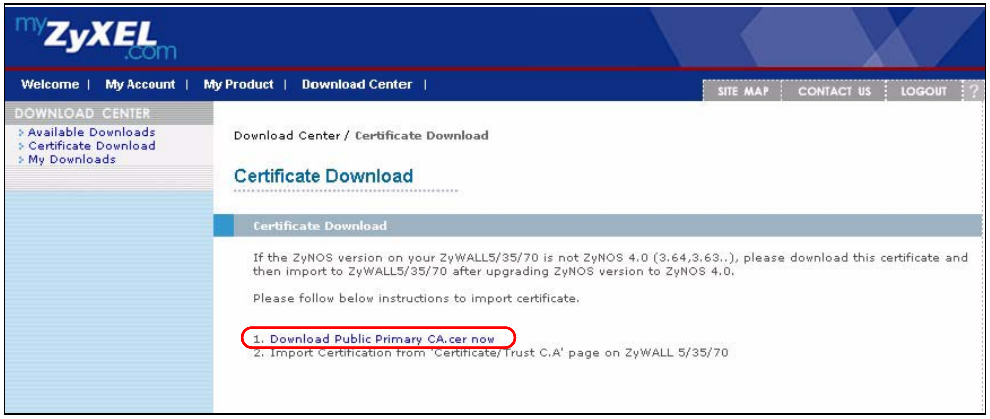
Last Viewed
* IP: 172.23.23.25
* Viewed Date: 2005/08/03
* Viewed time: 11:54:54(GMT+8:00)Taipei

Click here to register product

Note:
Currently, this registration website http://www.myzyxel.com supports Vantage CNM 2.0 and ZyXEL products service activation.
For other products support, we will announce soon in our next release.

3 Click the link in the **Certificate Download** screen.

**Figure 273** myZyXEL.com: Certificate Download


myZyXEL.com
Welcome | My Account | My Product | Download Center |
SITE MAP
CONTACT US
LOGOUT
?
DOWNLOAD CENTER
Available Downloads
Certificate Download
My Downloads
Download Center / Certificate Download
Certificate Download
Certificate Download

If the ZyNOS version on your ZyWALL5/35/70 is not ZyNOS 4.0 (3.64,3.63..), please download this certificate and then import to ZyWALL5/35/70 after upgrading ZyNOS version to ZyNOS 4.0.

Please follow below instructions to import certificate.

1. Download Public Primary CA.cer now
2. Import Certification from 'Certificate/Trust C.A' page on ZyWALL 5/35/70

## 25.3 Configuring Log Settings

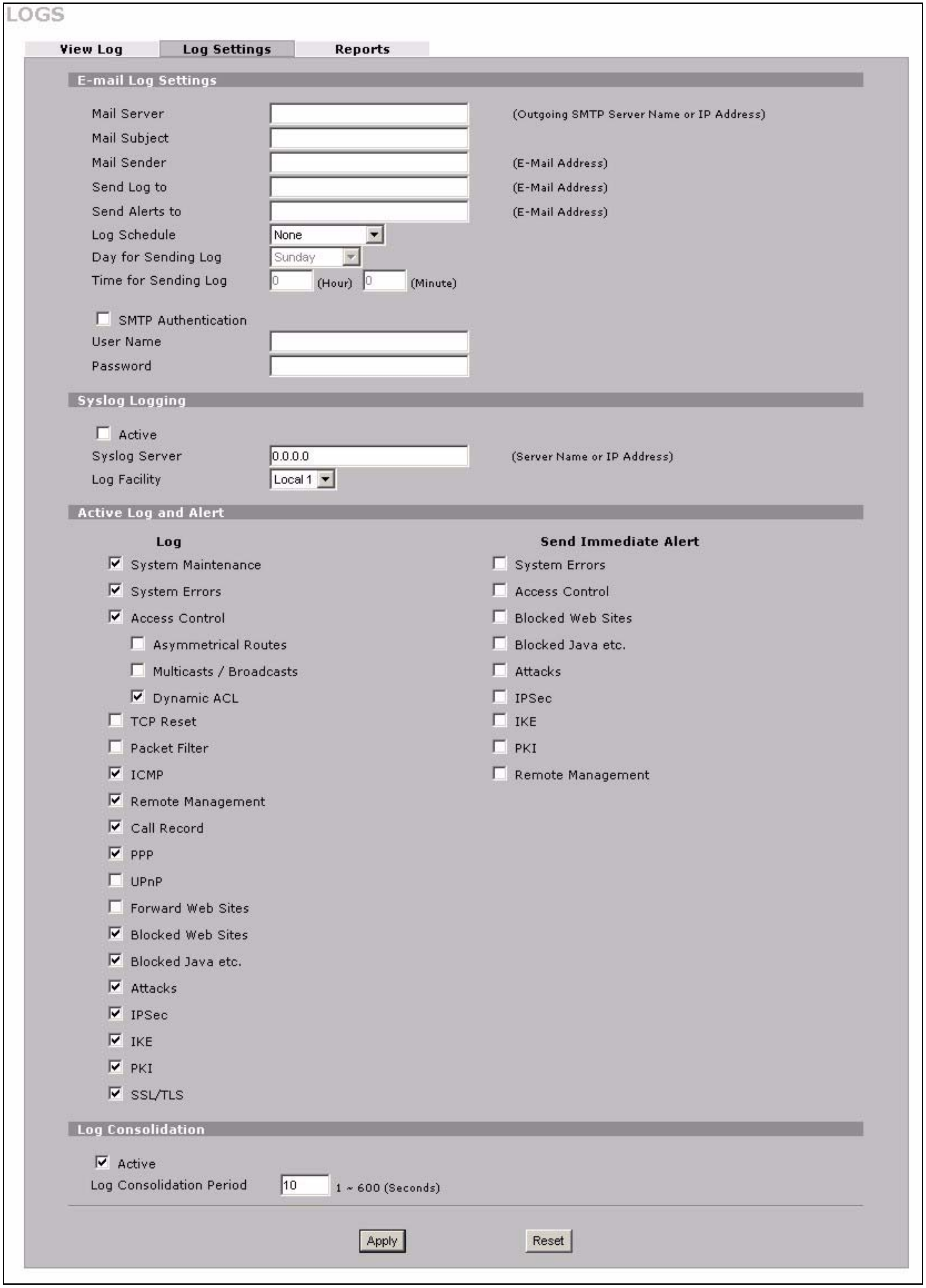
To change your ZyWALL’s log settings, click **LOGS** > **Log Settings**. The screen appears as shown.

Use the **Log Settings** screen to configure to where the ZyWALL is to send logs; the schedule for when the ZyWALL is to send the logs and which logs and/or immediate alerts the ZyWALL is to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

**Figure 274** LOGS > Log Settings



E-mail Log Settings

Mail Server (Outgoing SMTP Server Name or IP Address)
Mail Subject
Mail Sender (E-Mail Address)
Send Log to (E-Mail Address)
Send Alerts to (E-Mail Address)
Log Schedule: None
Day for Sending Log: Sunday
Time for Sending Log: 0 (Hour) 0 (Minute)

☐ SMTP Authentication
User Name
Password

Syslog Logging

☐ Active
Syslog Server: 0.0.0.0 (Server Name or IP Address)
Log Facility: Local 1

Active Log and Alert

Log
- ☑ System Maintenance
- ☑ System Errors
- ☑ Access Control
  - ☐ Asymmetrical Routes
  - ☐ Multicasts / Broadcasts
  - ☑ Dynamic ACL
- ☐ TCP Reset
- ☐ Packet Filter
- ☑ ICMP
- ☑ Remote Management
- ☑ Call Record
- ☑ PPP
- ☐ UPnP
- ☐ Forward Web Sites
- ☑ Blocked Web Sites
- ☑ Blocked Java etc.
- ☑ Attacks
- ☑ IPSec
- ☑ IKE
- ☑ PKI
- ☑ SSL/TLS

Send Immediate Alert
- ☐ System Errors
- ☐ Access Control
- ☐ Blocked Web Sites
- ☐ Blocked Java etc.
- ☐ Attacks
- ☐ IPSec
- ☐ IKE
- ☐ PKI
- ☐ Remote Management

Log Consolidation

☑ Active
Log Consolidation Period: 10 1 ~ 600 (Seconds)

The following table describes the labels in this screen.

**Table 134** LOGS > Log Settings

| LABEL | DESCRIPTION |
|---|---|
| E-mail Log Settings | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail. |
| Mail Subject | Type a title that you want to be in the subject line of the log e-mail message that the ZyWALL sends. |
| Mail Sender | Enter the e-mail address that you want to be in the from/sender line of the log e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well. |
| Send Log To | Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail. |
| Send Alerts To | Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail. |
| Log Schedule | This drop-down menu is used to configure the frequency of log messages being sent as E-mail:<br>**Daily**<br>**Weekly**<br>**Hourly**<br>**When Log is Full**<br>**None**.<br>If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent. |
| Day for Sending Log | Use the drop down list box to select which day of the week to send the logs. |
| Time for Sending Log | Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs. |
| SMTP Authentication | SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.<br>Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs. |
| User Name | Enter the user name (up to 31 characters) (usually the user name of a mail account). |
| Password | Enter the password associated with the user name above. |
| Syslog Logging | Syslog allows you to send system logs to a server.<br>Syslog logging sends a log to an external syslog server. |
| Active | Click **Active** to enable syslog logging. |
| Syslog Server | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |
| Log Facility | Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Active Log and Alert | |
| Log | Select the categories of logs that you want to record. Logs include alerts. |

**Table 134** LOGS > Log Settings (continued)

| LABEL | DESCRIPTION |
|---|---|
| Send Immediate Alert | Select the categories of alerts for which you want the ZyWALL to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field. |
| Log Consolidation | |
| Active | Some logs (such as the Attacks logs) may be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log.<br>You can use the `sys log consolidate msglist` command to see what log messages will be consolidated. |
| Log Consolidation Period | Specify the time interval during which the ZyWALL merges logs with identical messages into one log. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 25.4 Configuring Reports

The **Reports** screen displays which computers on the LAN, DMZ or WLAN send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. The ZyWALL can record and display the following network usage details:

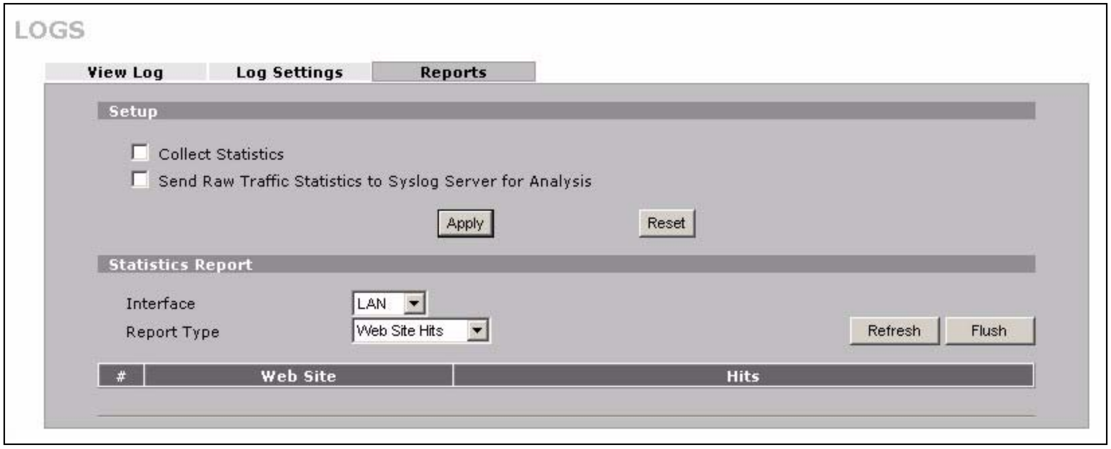
- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN, DMZ or WLAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the LAN, DMZ or WLAN IP addresses to and/or from which the most traffic has been sent

The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

The ZyWALL records web site hits by counting the HTTP GET packets. Many web sites include HTTP GET references to other web sites and the ZyWALL may count these as hits, thus the web hit count is not (yet) 100% accurate.

Click **LOGS** > **Reports** to display the following screen.

**Figure 275** LOGS > Reports


LOGS
View Log
Log Settings
Reports
Setup
☐ Collect Statistics
☐ Send Raw Traffic Statistics to Syslog Server for Analysis
Apply
Reset
Statistics Report
Interface
LAN
Report Type
Web Site Hits
Refresh
Flush
#
Web Site
Hits

Enabling the ZyWALL's reporting function decreases the overall throughput by about 1 Mbps.

The following table describes the labels in this screen.

**Table 135** LOGS > Reports

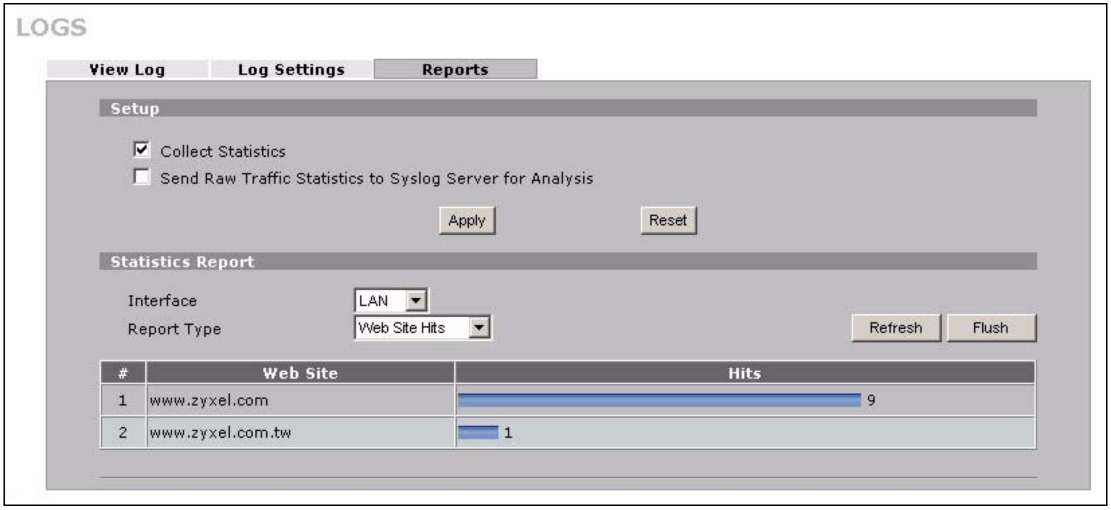
| LABEL | DESCRIPTION |
|---|---|
| Collect Statistics | Select the check box and click **Apply** to have the ZyWALL record report data. |
| Send Raw Traffic Statistics to Syslog Server for Analysis | Select the check box and click **Apply** to have the ZyWALL send unprocessed traffic statistics to a syslog server for analysis.<br>You must have the syslog server already configured in the **Log Settings** screen. |
| Apply | Click **Apply** to save your changes to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| Interface | Select on which interface (**LAN**, **DMZ** or **WLAN**) the logs will be collected. The logs on the DMZ, LAN or WLAN IP alias 1 and 2 are also recorded. |
| Report Type | Use the drop-down list box to select the type of reports to display.<br>**Web Site Hits** displays the web sites that have been visited the most often from the LAN and how many times they have been visited.<br>**Protocol/Port** displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports.<br>**Host IP Address** displays the LAN, DMZ or WLAN IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses. |
| Refresh | Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen. |
| Flush | Click **Flush** to discard the old report data and update the report display. |

All of the recorded reports data is erased when you turn off the ZyWALL.

## 25.4.1 Viewing Web Site Hits

In the **Reports** screen, select **Web Site Hits** from the **Report Type** drop-down list box to have the ZyWALL record and display which web sites have been visited the most often and how many times they have been visited.

**Figure 276** LOGS > Reports: Web Site Hits Example



☑ Collect Statistics
☐ Send Raw Traffic Statistics to Syslog Server for Analysis

Interface: LAN
Report Type: Web Site Hits

| # | Web Site | Hits |
|---|---|---|
| 1 | www.zyxel.com | 9 |
| 2 | www.zyxel.com.tw | 1 |

The following table describes the label in this screen.

**Table 136** LOGS > Reports: Web Site Hits Report

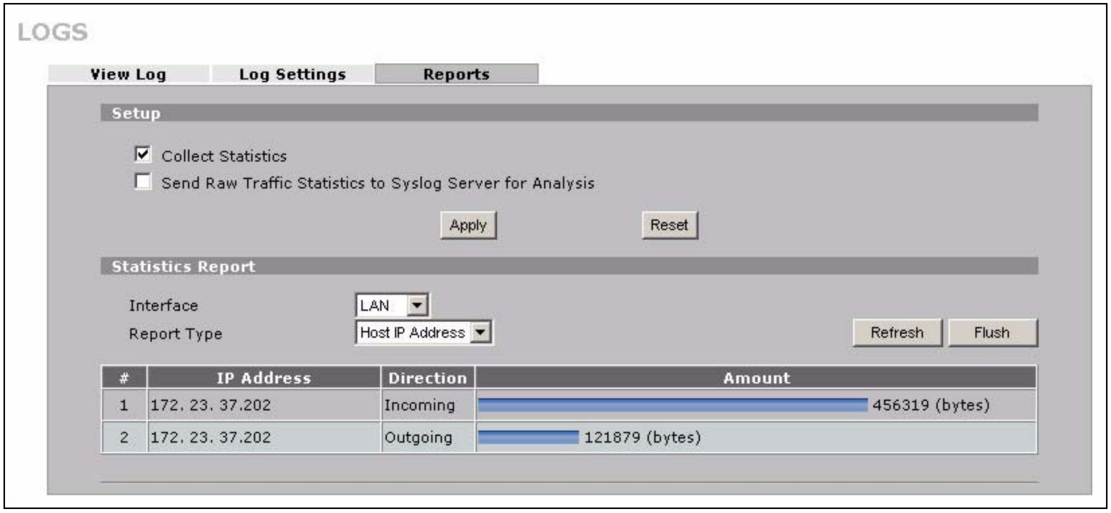
| LABEL | DESCRIPTION |
|---|---|
| Web Site | This column lists the domain names of the web sites visited most often from computers on the LAN, DMZ or WLAN. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The ZyWALL counts each page viewed in a web site as another hit on the web site. |
| Hits | This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit (see Table 139 on page 430). |

## 25.4.2 Viewing Host IP Address

In the **Reports** screen, select **Host IP Address** from the **Report Type** drop-down list box to have the ZyWALL record and display the LAN, DMZ or WLAN IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.

Computers take turns using dynamically assigned LAN, DMZ or WLAN IP addresses. The ZyWALL continues recording the bytes sent to or from a LAN, DMZ or WLAN IP address when it is assigned to a different computer.

**Figure 277** LOGS > Reports: Host IP Address Example



☑ Collect Statistics
☐ Send Raw Traffic Statistics to Syslog Server for Analysis

Interface: LAN
Report Type: Host IP Address

| # | IP Address | Direction | Amount |
|---|---|---|---|
| 1 | 172. 23. 37.202 | Incoming | 456319 (bytes) |
| 2 | 172. 23. 37.202 | Outgoing | 121879 (bytes) |

The following table describes the labels in this screen.

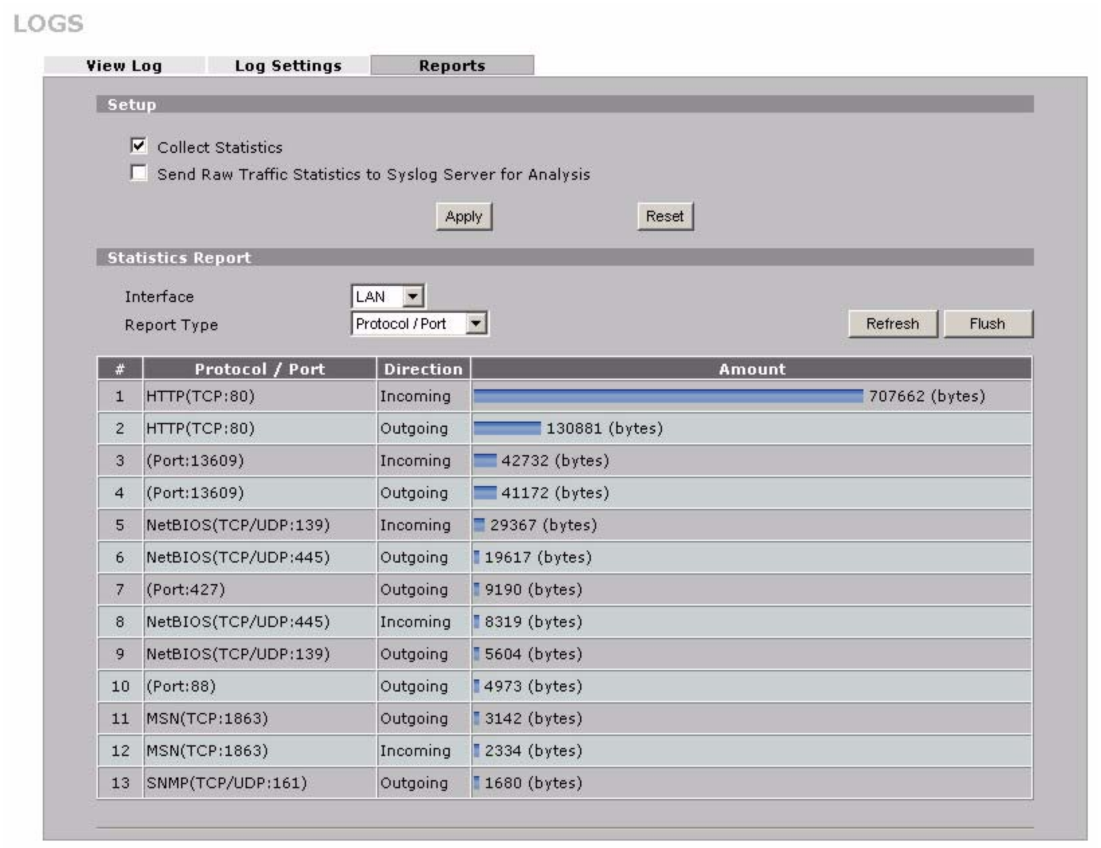
**Table 137** LOGS > Reports: Host IP Address

| LABEL | DESCRIPTION |
|---|---|
| IP Address | This column lists the LAN, DMZ or WLAN IP addresses to and/or from which the most traffic has been sent. The LAN, DMZ or WLAN IP addresses are listed in descending order with the LAN, DMZ or WLAN IP address to and/or from which the most traffic was sent listed first. |
| Direction | This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN, DMZ or WLAN. This field displays **Outgoing** to denote traffic that is going out from the LAN, DMZ or WLAN to the WAN. |
| Amount | This column displays how much traffic has gone to and from the listed LAN, DMZ or WLAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN, DMZ or WLAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN, DMZ or WLAN IP passes the bytes count limit (see Table 139 on page 430). |

## 25.4.3 Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list box to have the ZyWALL record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

**Figure 278** LOGS > Reports: Protocol/Port Example



☑ Collect Statistics
☐ Send Raw Traffic Statistics to Syslog Server for Analysis

Interface: LAN
Report Type: Protocol / Port

| # | Protocol / Port | Direction | Amount |
|---|---|---|---|
| 1 | HTTP(TCP:80) | Incoming | 707662 (bytes) |
| 2 | HTTP(TCP:80) | Outgoing | 130881 (bytes) |
| 3 | (Port:13609) | Incoming | 42732 (bytes) |
| 4 | (Port:13609) | Outgoing | 41172 (bytes) |
| 5 | NetBIOS(TCP/UDP:139) | Incoming | 29367 (bytes) |
| 6 | NetBIOS(TCP/UDP:445) | Outgoing | 19617 (bytes) |
| 7 | (Port:427) | Outgoing | 9190 (bytes) |
| 8 | NetBIOS(TCP/UDP:445) | Incoming | 8319 (bytes) |
| 9 | NetBIOS(TCP/UDP:139) | Outgoing | 5604 (bytes) |
| 10 | (Port:88) | Outgoing | 4973 (bytes) |
| 11 | MSN(TCP:1863) | Outgoing | 3142 (bytes) |
| 12 | MSN(TCP:1863) | Incoming | 2334 (bytes) |
| 13 | SNMP(TCP/UDP:161) | Outgoing | 1680 (bytes) |

The following table describes the labels in this screen.

**Table 138** LOGS > Reports: Protocol/ Port

| LABEL | DESCRIPTION |
|---|---|
| Protocol/Port | This column lists the protocols or service ports for which the most traffic has gone through the ZyWALL. The protocols or service ports are listed in descending order with the most used protocol or service port listed first. |
| Direction | This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN, DMZ or WLAN. This field displays **Outgoing** to denote traffic that is going out from the LAN, DMZ or WLAN to the WAN. |
| Amount | This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see Table 139 on page 430). |

### 25.4.4 System Reports Specifications

The following table lists detailed specifications on the reports feature.

**Table 139** Report Specifications

| LABEL | DESCRIPTION |
|---|---|
| Number of web sites/protocols or ports/IP addresses listed: | 20 |
| Hit count limit: | Up to $2^{32}$ hits can be counted per web site. The count starts over at 0 if it passes four billion. |
| Bytes count limit: | Up to $2^{64}$ bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes $2^{64}$ bytes. |

## 25.5 Log Descriptions

This section provides descriptions of example log messages.

**Table 140** System Maintenance Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Time calibration is successful` | The router has adjusted its time based on information from the time server. |
| `Time calibration failed` | The router failed to get information from the time server. |
| `WAN interface gets IP: %s` | A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server. |
| `DHCP client IP expired` | A DHCP client's IP address has expired. |
| `DHCP server assigns %s` | The DHCP server assigned an IP address to a client. |
| `Successful SMT login` | Someone has logged on to the router's SMT interface. |
| `SMT login failed` | Someone has failed to log on to the router's SMT interface. |
| `Successful WEB login` | Someone has logged on to the router's web configurator interface. |
| `WEB login failed` | Someone has failed to log on to the router's web configurator interface. |
| `Successful TELNET login` | Someone has logged on to the router via telnet. |
| `TELNET login failed` | Someone has failed to log on to the router via telnet. |
| `Successful FTP login` | Someone has logged on to the router via FTP. |
| `FTP login failed` | Someone has failed to log on to the router via FTP. |
| `NAT Session Table is Full!` | The maximum number of NAT session table entries has been exceeded and the table is full. |
| `Starting Connectivity Monitor` | Starting Connectivity Monitor. |
| `Time initialized by Daytime Server` | The router got the time and date from the Daytime server. |
| `Time initialized by Time server` | The router got the time and date from the time server. |

**Table 140** System Maintenance Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Time initialized by NTP server` | The router got the time and date from the NTP server. |
| `Connect to Daytime server fail` | The router was not able to connect to the Daytime server. |
| `Connect to Time server fail` | The router was not able to connect to the Time server. |
| `Connect to NTP server fail` | The router was not able to connect to the NTP server. |
| `Too large ICMP packet has been dropped` | The router dropped an ICMP packet that was too large. |
| `SMT Session Begin` | An SMT management session has started. |
| `SMT Session End` | An SMT management session has ended. |
| `Configuration Change: PC = 0x%x, Task ID = 0x%x` | The router is saving configuration changes. |
| `Successful SSH login` | Someone has logged on to the router’s SSH server. |
| `SSH login failed` | Someone has failed to log on to the router’s SSH server. |
| `Successful HTTPS login` | Someone has logged on to the router's web configurator interface using HTTPS protocol. |
| `HTTPS login failed` | Someone has failed to log on to the router's web configurator interface using HTTPS protocol. |
| `DNS server %s was not responding to last 32 consecutive queries…` | The specified DNS server did not respond to the last 32 consecutive queries. |
| `DDNS update IP:%s (host %d) successfully` | The device updated the IP address of the specified DDNS host name. |
| `SMTP successfully` | The device sent an e-mail. |
| `myZyXEL.com registration successful` | Registration of the device with myZyXEL.com was successful. |
| `Trial service registration successful` | Registration for a trial service was successful. |
| `Service upgrade successful` | Registration for a service upgrade was successful. |
| `Service refresh successful.` | The device successfully refreshed service information from myZyXEL.com. |
| `Content Filter trial service activation successfully` | The content filtering trial service was successfully activated for this device. |
| `%s` | The myZyXEL.com service registration failed due to the error listed. If you are unable to register for services at myZYXEL.com, the error message displayed in this log may be useful when contacting customer support. |

**Table 141** System Error Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `%s exceeds the max. number of session per host!` | This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host. |
| `setNetBIOSFilter: calloc error` | The router failed to allocate memory for the NetBIOS filter settings. |
| `readNetBIOSFilter: calloc error` | The router failed to allocate memory for the NetBIOS filter settings. |
| `WAN connection is down.` | A WAN connection is down. You cannot access the network through this interface. |
| `Dial Backup starts` | Dial backup started working. |
| `Dial Backup ends` | Dial backup stopped working. |
| `DHCP Server cannot assign the static IP %S (out of range).` | The LAN subnet, LAN alias 1, or LAN alias 2 was changed and the specified static DHCP IP addresses are no longer valid. |
| `The DHCP static IP %s is conflict.` | The static DHCP IP address conflicts with another host. |
| `SMTP fail (%s)` | The device failed to send an e-mail (error message included). |
| `SMTP authentication fail (%s)` | The device failed to authenticate with the SMTP server (error message included). |

**Table 142** Access Control Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Firewall default policy: [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] <Packet Direction>` | Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy’s setting. |
| `Firewall rule [NOT] match:[ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] <Packet Direction>, <rule:%d>` | Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule. |
| `Triangle route packet forwarded: [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ]` | The firewall allowed a triangle route session to pass through. |
| `Packet without a NAT table entry blocked: [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ]` | The router blocked a packet that didn't have a corresponding NAT table entry. |
| `Router sent blocked web site message: TCP` | The router sent a message to notify a user that the router blocked access to a web site that the user requested. |
| `Exceed maximum sessions per host (%d).` | The device blocked a session because the host's connections exceeded the maximum sessions per host. |
| `Firewall allowed a packet that matched a NAT session: [ TCP \| UDP ]` | A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN. |

**Table 143** TCP Reset Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Under SYN flood attack, sent TCP RST` | The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.) |
| `Exceed TCP MAX incomplete, sent TCP RST` | The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen. |
| `Peer TCP state out of order, sent TCP RST` | The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state. |
| `Firewall session time out, sent TCP RST` | The router sent a TCP reset packet when a dynamic firewall session timed out.<br>The default timeout values are as follows:<br>ICMP idle timeout: 3 minutes<br>UDP idle timeout: 3 minutes<br>TCP connection (three way handshaking) timeout: 270 seconds<br>TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header).<br>TCP idle (established) timeout (s): 150 minutes<br>TCP reset timeout: 10 seconds |
| `Exceed MAX incomplete, sent TCP RST` | The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”. |
| `Access block, sent TCP RST` | The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst"). |

**Table 144** Packet Filter Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `[ TCP \| UDP \| ICMP \| IGMP \| Generic ] packet filter matched (set: %d, rule: %d)` | Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule. |

For type and code details, see Table 157 on page 443.

**Table 145** ICMP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>` | ICMP access matched the default policy and was blocked or forwarded according to the user's setting. |
| `Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>` | ICMP access matched (or didn’t match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. |
| `Triangle route packet forwarded: ICMP` | The firewall allowed a triangle route session to pass through. |

**Table 145** ICMP Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Packet without a NAT table entry blocked: ICMP` | The router blocked a packet that didn't have a corresponding NAT table entry. |
| `Unsupported/out-of-order ICMP: ICMP` | The firewall does not support this kind of ICMP packets or the ICMP packets are out of order. |
| `Router reply ICMP packet: ICMP` | The router sent an ICMP reply packet to the sender. |

**Table 146** CDR Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s` | The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID. For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times. |
| `board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s` | The PPPoE, PPTP or dial-up call is connected. |
| `board %d line %d channel %d, call %d, %s C02 Call Terminated` | The PPPoE, PPTP or dial-up call was disconnected. |

**Table 147** PPP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `ppp:LCP Starting` | The PPP connection's Link Control Protocol stage has started. |
| `ppp:LCP Opening` | The PPP connection's Link Control Protocol stage is opening. |
| `ppp:CHAP Opening` | The PPP connection's Challenge Handshake Authentication Protocol stage is opening. |
| `ppp:IPCP Starting` | The PPP connection's Internet Protocol Control Protocol stage is starting. |
| `ppp:IPCP Opening` | The PPP connection's Internet Protocol Control Protocol stage is opening. |
| `ppp:LCP Closing` | The PPP connection's Link Control Protocol stage is closing. |
| `ppp:IPCP Closing` | The PPP connection's Internet Protocol Control Protocol stage is closing. |

**Table 148** UPnP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `UPnP pass through Firewall` | UPnP packets can pass through the firewall. |

**Table 149** Content Filtering Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `%s: Keyword blocking` | The content of a requested web page matched a user defined keyword. |
| `%s: Not in trusted web list` | The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites. |
| `%s: Forbidden Web site` | The web site is in the forbidden web site list. |
| `%s: Contains ActiveX` | The web site contains ActiveX. |
| `%s: Contains Java applet` | The web site contains a Java applet. |
| `%s: Contains cookie` | The web site contains a cookie. |
| `%s: Proxy mode detected` | The router detected proxy mode in the packet. |
| `%s` | The content filter server responded that the web site is in the blocked category list, but it did not return the category type. |
| `%s: %s` | The content filter server responded that the web site is in the blocked category list, and returned the category type. |
| `%s(cache hit)` | The system detected that the web site is in the blocked list from the local cache, but does not know the category type. |
| `%s :%s(cache hit)` | The system detected that the web site is in blocked list from the local cache, and knows the category type. |
| `%s: Trusted Web site` | The web site is in a trusted domain. |
| `%s` | When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" check box, the system forwards the web content. |
| `Waiting content filter server timeout` | The external content filtering server did not respond within the timeout period. |
| `DNS resolving failed` | The ZyWALL cannot get the IP address of the external content filtering via DNS query. |
| `Creating socket failed` | The ZyWALL cannot issue a query because TCP/IP socket creation failed, port:port number. |
| `Connecting to content filter server fail` | The connection to the external content filtering server failed. |
| `License key is invalid` | The external content filtering license key is invalid. |

For type and code details, see Table 157 on page 443.

**Table 150** Attack Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `attack [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ]` | The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack. |
| `attack ICMP (type:%d, code:%d)` | The firewall detected an ICMP attack. |
| `land [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ]` | The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack. |
| `land ICMP (type:%d, code:%d)` | The firewall detected an ICMP land attack. |

**Table 150** Attack Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `ip spoofing - WAN [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ]` | The firewall detected an IP spoofing attack on the WAN port. |
| `ip spoofing - WAN ICMP (type:%d, code:%d)` | The firewall detected an ICMP IP spoofing attack on the WAN port. |
| `icmp echo : ICMP (type:%d, code:%d)` | The firewall detected an ICMP echo attack. |
| `syn flood TCP` | The firewall detected a TCP syn flood attack. |
| `ports scan TCP` | The firewall detected a TCP port scan attack. |
| `teardrop TCP` | The firewall detected a TCP teardrop attack. |
| `teardrop UDP` | The firewall detected an UDP teardrop attack. |
| `teardrop ICMP (type:%d, code:%d)` | The firewall detected an ICMP teardrop attack. |
| `illegal command TCP` | The firewall detected a TCP illegal command attack. |
| `NetBIOS TCP` | The firewall detected a TCP NetBIOS attack. |
| `ip spoofing - no routing entry [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ]` | The firewall classified a packet with no source routing entry as an IP spoofing attack. |
| `ip spoofing - no routing entry ICMP (type:%d, code:%d)` | The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack. |
| `vulnerability ICMP (type:%d, code:%d)` | The firewall detected an ICMP vulnerability attack. |
| `traceroute ICMP (type:%d, code:%d)` | The firewall detected an ICMP traceroute attack. |
| `ports scan UDP` | The firewall detected a UDP port scan attack. |
| `Firewall sent TCP packet in response to DoS attack TCP` | The firewall sent TCP packet in response to a DoS attack |
| `ICMP Source Quench ICMP` | The firewall detected an ICMP Source Quench attack. |
| `ICMP Time Exceed ICMP` | The firewall detected an ICMP Time Exceed attack. |
| `ICMP Destination Unreachable ICMP` | The firewall detected an ICMP Destination Unreachable attack. |
| `ping of death. ICMP` | The firewall detected an ICMP ping of death attack. |
| `smurf ICMP` | The firewall detected an ICMP smurf attack. |
| `IP address in FTP port command is different from the client IP address. It maybe a bounce attack.` | The IP address in an FTP port command is different from the client IP address. It may be a bounce attack. |
| `Fragment packet size is smaller than the MTU size of output interface.` | The fragment packet size is smaller than the MTU size of output interface. |

**Table 151** Remote Management Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Remote Management: FTP denied` | Attempted use of FTP service was blocked according to remote management settings. |
| `Remote Management: TELNET denied` | Attempted use of TELNET service was blocked according to remote management settings. |
| `Remote Management: HTTP or UPnP denied` | Attempted use of HTTP or UPnP service was blocked according to remote management settings. |
| `Remote Management: WWW denied` | Attempted use of WWW service was blocked according to remote management settings. |
| `Remote Management: HTTPS denied` | Attempted use of HTTPS service was blocked according to remote management settings. |
| `Remote Management: SSH denied` | Attempted use of SSH service was blocked according to remote management settings. |
| `Remote Management: ICMP Ping response denied` | Attempted use of ICMP service was blocked according to remote management settings. |
| `Remote Management: SNMP denied` | Attempted use of SNMP service was blocked according to remote management settings. |
| `Remote Management: DNS denied` | Attempted use of DNS service was blocked according to remote management settings. |

**Table 152** IPSec Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Discard REPLAY packet` | The router received and discarded a packet with an incorrect sequence number. |
| `Inbound packet authentication failed` | The router received a packet that has been altered. A third party may have altered or tampered with the packet. |
| `Receive IPSec packet, but no corresponding tunnel exists` | The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA. |
| `Rule <%d> idle time out, disconnect` | The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes. |
| `WAN IP changed to <IP>` | The router dropped all connections with the “MyIP” configured as “0.0.0.0” when the WAN IP address changed. |
| `Inbound packet decryption failed` | Please check the algorithm configuration. |
| `Cannot find outbound SA for rule <%d>` | A packet matches a rule, but there is no phase 2 SA for outbound traffic. |
| `Rule [%s] sends an echo request to peer` | The device sent a ping packet to check the specified VPN tunnel's connectivity. |
| `Rule [%s] receives an echo reply from peer` | The device received a ping response when checking the specified VPN tunnel's connectivity. |

**Table 153** IKE Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Active connection allowed exceeded` | The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached. |
| `Start Phase 2: Quick Mode` | Phase 2 Quick Mode has started. |
| `Verifying Remote ID failed:` | The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match. |
| `Verifying Local ID failed:` | The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match. |
| `IKE Packet Retransmit` | The router retransmitted the last packet sent because there was no response from the peer. |
| `Failed to send IKE Packet` | An Ethernet error stopped the router from sending IKE packets. |
| `Too many errors! Deleting SA` | An SA was deleted because there were too many errors. |
| `Phase 1 IKE SA process done` | The phase 1 IKE SA process has been completed. |
| `Duplicate requests with the same cookie` | The router received multiple requests from the same peer while still processing the first IKE packet from the peer. |
| `IKE Negotiation is in process` | The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet. |
| `No proposal chosen` | Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail. |
| `Local / remote IPs of incoming request conflict with rule <%d>` | The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed. |
| `Cannot resolve Secure Gateway Addr for rule <%d>` | The router couldn't resolve the IP address from the domain name that was used for the secure gateway address. |
| `Peer ID: <peer id> <My remote type> -<My local type>` | The displayed ID information did not match between the two ends of the connection. |
| `vs. My Remote <My remote> - <My remote>` | The displayed ID information did not match between the two ends of the connection. |
| `vs. My Local <My local>-<My local>` | The displayed ID information did not match between the two ends of the connection. |
| `Send <packet>` | A packet was sent. |
| `Recv <packet>` | IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types. |
| `Recv <Main or Aggressive> Mode request from <IP>` | The router received an IKE negotiation request from the peer address specified. |
| `Send <Main or Aggressive> Mode request to <IP>` | The router started negotiation with the peer. |
| `Invalid IP <Peer local> / <Peer local>` | The peer's "Local IP Address" is invalid. |

**Table 153** IKE Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Remote IP <Remote IP> / <Remote IP> conflicts` | The security gateway is set to “0.0.0.0” and the router used the peer’s “Local Address” as the router’s “Remote Address”. This information conflicted with static rule #d; thus the connection is not allowed. |
| `Phase 1 ID type mismatch` | This router’s "Peer ID Type" is different from the peer IPSec router's "Local ID Type". |
| `Phase 1 ID content mismatch` | This router’s "Peer ID Content" is different from the peer IPSec router's "Local ID Content". |
| `No known phase 1 ID type found` | The router could not find a known phase 1 ID in the connection attempt. |
| `ID type mismatch. Local / Peer: <Local ID type/Peer ID type>` | The phase 1 ID types do not match. |
| `ID content mismatch` | The phase 1 ID contents do not match. |
| `Configured Peer ID Content: <Configured Peer ID Content>` | The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed. |
| `Incoming ID Content: <Incoming Peer ID Content>` | The phase 1 ID contents do not match and the incoming packet's ID content is displayed. |
| `Unsupported local ID Type: <%d>` | The phase 1 ID type is not supported by the router. |
| `Build Phase 1 ID` | The router has started to build the phase 1 ID. |
| `Adjust TCP MSS to %d` | The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel. |
| `Rule <%d> input idle time out, disconnect` | The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period. |
| `XAUTH succeed! Username: <Username>` | The router used extended authentication to authenticate the listed username. |
| `XAUTH fail! Username: <Username>` | The router was not able to use extended authentication to authenticate the listed username. |
| `Rule[%d] Phase 1 negotiation mode mismatch` | The listed rule’s IKE phase 1 negotiation mode did not match between the router and the peer. |
| `Rule [%d] Phase 1 encryption algorithm mismatch` | The listed rule’s IKE phase 1 encryption algorithm did not match between the router and the peer. |
| `Rule [%d] Phase 1 authentication algorithm mismatch` | The listed rule’s IKE phase 1 authentication algorithm did not match between the router and the peer. |
| `Rule [%d] Phase 1 authentication method mismatch` | The listed rule’s IKE phase 1 authentication method did not match between the router and the peer. |
| `Rule [%d] Phase 1 key group mismatch` | The listed rule’s IKE phase 1 key group did not match between the router and the peer. |
| `Rule [%d] Phase 2 protocol mismatch` | The listed rule’s IKE phase 2 protocol did not match between the router and the peer. |
| `Rule [%d] Phase 2 encryption algorithm mismatch` | The listed rule’s IKE phase 2 encryption algorithm did not match between the router and the peer. |

**Table 153** IKE Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Rule [%d] Phase 2 authentication algorithm mismatch` | The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer. |
| `Rule [%d] Phase 2 encapsulation mismatch` | The listed rule's IKE phase 2 encapsulation did not match between the router and the peer. |
| `Rule [%d]> Phase 2 pfs mismatch` | The listed rule's IKE phase 2 perfect forward secret (PFS) setting did not match between the router and the peer. |
| `Rule [%d] Phase 1 ID mismatch` | The listed rule's IKE phase 1 ID did not match between the router and the peer. |
| `Rule [%d] Phase 1 hash mismatch` | The listed rule's IKE phase 1 hash did not match between the router and the peer. |
| `Rule [%d] Phase 1 preshared key mismatch` | The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer. |
| `Rule [%d] Tunnel built successfully` | The listed rule's IPSec tunnel has been built successfully. |
| `Rule [%d] Peer's public key not found` | The listed rule's IKE phase 1 peer's public key was not found. |
| `Rule [%d] Verify peer's signature failed` | The listed rule's IKE phase 1verification of the peer's signature failed. |
| `Rule [%d] Sending IKE request` | IKE sent an IKE request for the listed rule. |
| `Rule [%d] Receiving IKE request` | IKE received an IKE request for the listed rule. |
| `Swap rule to rule [%d]` | The router changed to using the listed rule. |
| `Rule [%d] Phase 1 key length mismatch` | The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer. |
| `Rule [%d] phase 1 mismatch` | The listed rule's IKE phase 1 did not match between the router and the peer. |
| `Rule [%d] phase 2 mismatch` | The listed rule's IKE phase 2 did not match between the router and the peer. |
| `Rule [%d] Phase 2 key length mismatch` | The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer. |
| `Remote Gateway Addr in rule [%s] is changed to %s"` | The IP address for the domain name of the peer gateway in the listed rule changed to the listed IP address. |
| `New My ZyWALL Addr in rule [%s] is changed to %s` | The IP address for the domain name of the ZyWALL in the listed rule changed to the listed IP address. |
| `Remote Gateway Addr has changed, tunnel [%s] will be deleted` | The listed tunnel will be deleted because the remote gateway's IP address changed. |
| `My ZyWALL Addr has changed, tunnel [%s] will be deleted` | The listed tunnel will be deleted because the ZyWALL's IP address changed. |

**Table 154** PKI Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Enrollment successful` | The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port. |
| `Enrollment failed` | The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port. |
| `Failed to resolve <SCEP CA server url>` | The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved. |
| `Enrollment successful` | The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port. |
| `Enrollment failed` | The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port. |
| `Failed to resolve <CMP CA server url>` | The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved. |
| `Rcvd ca cert: <subject name>` | The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field. |
| `Rcvd user cert: <subject name>` | The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field. |
| `Rcvd CRL <size>: <issuer name>` | The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field. |
| `Rcvd ARL <size>: <issuer name>` | The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field. |
| `Failed to decode the received ca cert` | The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field. |
| `Failed to decode the received user cert` | The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field. |
| `Failed to decode the received CRL` | The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field. |
| `Failed to decode the received ARL` | The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field. |
| `Rcvd data <size> too large! Max size allowed: <max size>` | The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded. |
| `Cert trusted: <subject name>` | The router has verified the path of the certificate with the listed subject name. |
| `Due to <reason codes>, cert not trusted: <subject name>` | Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 155 on page 442 for the corresponding descriptions of the codes. |

**Table 155** Certificate Path Verification Failure Reason Codes

| CODE | DESCRIPTION |
|---|---|
| 1 | Algorithm mismatch between the certificate and the search constraints. |
| 2 | Key usage mismatch between the certificate and the search constraints. |
| 3 | Certificate was not valid in the time interval. |
| 4 | (Not used) |
| 5 | Certificate is not valid. |
| 6 | Certificate signature was not verified correctly. |
| 7 | Certificate was revoked by a CRL. |
| 8 | Certificate was not added to the cache. |
| 9 | Certificate decoding failed. |
| 10 | Certificate was not found (anywhere). |
| 11 | Certificate chain looped (did not find trusted root). |
| 12 | Certificate contains critical extension that was not handled. |
| 13 | Certificate issuer was not valid (CA specific information missing). |
| 14 | (Not used) |
| 15 | CRL is too old. |
| 16 | CRL is not valid. |
| 17 | CRL signature was not verified correctly. |
| 18 | CRL was not found (anywhere). |
| 19 | CRL was not added to the cache. |
| 20 | CRL decoding failed. |
| 21 | CRL is not currently valid, but in the future. |
| 22 | CRL contains duplicate serial numbers. |
| 23 | Time interval is not continuous. |
| 24 | Time information not available. |
| 25 | Database method failed due to timeout. |
| 26 | Database method failed. |
| 27 | Path was not verified. |
| 28 | Maximum path length reached. |

**Table 156** ACL Setting Notes

| PACKET DIRECTION | DIRECTION | DESCRIPTION |
|---|---|---|
| (L to W) | LAN to WAN | ACL set for packets traveling from the LAN to the WAN. |
| (W to L) | WAN to LAN | ACL set for packets traveling from the WAN to the LAN. |
| (D to L) | DMZ to LAN | ACL set for packets traveling from the DMZ to the LAN. |
| (D to W) | DMZ to WAN | ACL set for packets traveling from the DMZ to the WAN. |
| (W to D) | WAN to DMZ | ACL set for packets traveling from the WAN to the DMZ. |
| (L to D) | LAN to DMZ | ACL set for packets traveling from the LAN to the DMZ. |

**Table 156** ACL Setting Notes (continued)

| PACKET DIRECTION | DIRECTION | DESCRIPTION |
|---|---|---|
| (L to L/ZW) | LAN to LAN/ ZyWALL | ACL set for packets traveling from the LAN to the LAN or the ZyWALL. |
| (W to W/ZW) | WAN to WAN/ ZyWALL | ACL set for packets traveling from the WAN to the WAN or the ZyWALL. |
| (D to D/ZW) | DMZ to DMZ/ ZyWALL | ACL set for packets traveling from the DMZ to the DM or the ZyWALL. |
| (L to WL) | LAN to WLAN | ACL set for packets traveling from the LAN to the WLAN. |
| (WL to L) | WLAN to LAN | ACL set for packets traveling from the WLAN to the LAN. |
| (W to WL) | WAN to WLAN | ACL set for packets traveling from the WAN to the WLAN. |
| (WL to W) | WLAN to WAN | ACL set for packets traveling from the WLAN to the WAN. |
| (D to WL) | DMZ to WLAN | ACL set for packets traveling from the DMZ to the WLAN. |
| (WL to D) | WLAN to DMZ | ACL set for packets traveling from the WLAN to the DMZ. |
| (WL to WL) | WLAN to WLAN/ ZyWALL | ACL set for packets traveling from the WLAN to the WLAN or the ZyWALL. |

**Table 157** ICMP Notes

| TYPE | CODE | DESCRIPTION |
|---|---|---|
| `0` | | Echo Reply |
| | `0` | Echo reply message |
| `3` | | Destination Unreachable |
| | `0` | Net unreachable |
| | `1` | Host unreachable |
| | `2` | Protocol unreachable |
| | `3` | Port unreachable |
| | `4` | A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF) |
| | `5` | Source route failed |
| `4` | | Source Quench |
| | `0` | A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network. |
| `5` | | Redirect |
| | `0` | Redirect datagrams for the Network |
| | `1` | Redirect datagrams for the Host |
| | `2` | Redirect datagrams for the Type of Service and Network |
| | `3` | Redirect datagrams for the Type of Service and Host |
| `8` | | Echo |
| | `0` | Echo message |
| `11` | | Time Exceeded |

**Table 157** ICMP Notes (continued)

| TYPE | CODE | DESCRIPTION |
|---|---|---|
| | 0 | Time to live exceeded in transit |
| | 1 | Fragment reassembly time exceeded |
| 12 | | Parameter Problem |
| | 0 | Pointer indicates the error |
| 13 | | Timestamp |
| | 0 | Timestamp request message |
| 14 | | Timestamp Reply |
| | 0 | Timestamp reply message |
| 15 | | Information Request |
| | 0 | Information request message |
| 16 | | Information Reply |
| | 0 | Information reply message |

## 25.6 Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

**Table 158** Syslog Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"` | This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs. |
| `Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/Normal"` | This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DMZ", "LAN:DEV" for example). |
| `Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0\|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"` | This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. OB is the Out Break flag and the mac address of the Out Break PC. |
| `Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="0\|1" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Virus" encode="< uu \| b64 >"` | This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The "encode" message indicates the mail attachments encoding method. The definition of messages and notes are defined in the Anti-Virus log descriptions. |

**Table 158** Syslog Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0\|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="IDP" class="<idp class>" sid="<idp sid> act="<idp action>" count="1"` | This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the IDP log descriptions. |
| `Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0\|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Spam" 1stReIP="<IP>"` | This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. 1stReIP is the IP address of the first mail relay server. The definition of messages and notes are defined in the Anti-Spam log descriptions. |

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

**Table 159** RFC-2408 ISAKMP Payload Types

| LOG DISPLAY | PAYLOAD TYPE |
|---|---|
| `SA` | Security Association |
| `PROP` | Proposal |
| `TRANS` | Transform |
| `KE` | Key Exchange |
| `ID` | Identification |
| `CER` | Certificate |
| `CER_REQ` | Certificate Request |
| `HASH` | Hash |
| `SIG` | Signature |
| `NONCE` | Nonce |
| `NOTFY` | Notification |
| `DEL` | Delete |
| `VID` | Vendor ID |

# 26

# Maintenance

This chapter displays information on the maintenance screens.

## 26.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyWALL.

## 26.2 General Setup and System Name

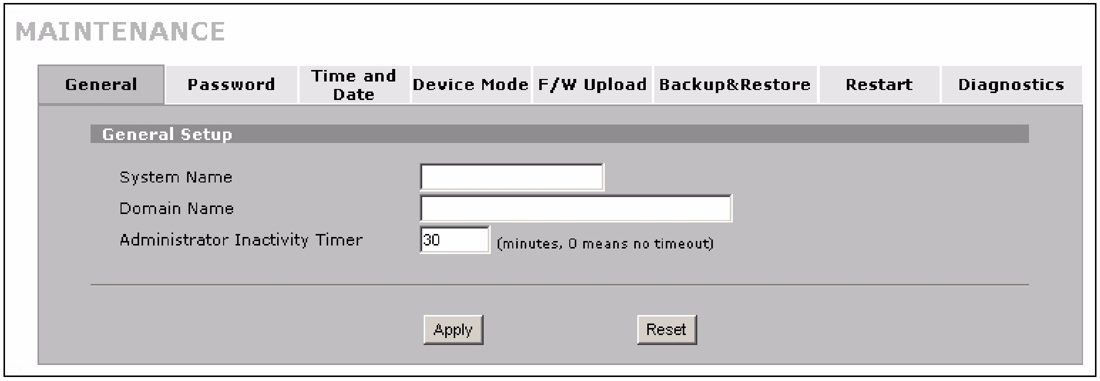
**General Setup** contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyWALL **System Name**.

### 26.2.1 General Setup

Click **MAINTENANCE** to open the **General** screen. Use this screen to configure administrative and system-related information.

**Figure 279** MAINTENANCE > General Setup



System Name
Domain Name
Administrator Inactivity Timer 30 (minutes, 0 means no timeout)

The following table describes the labels in this screen.

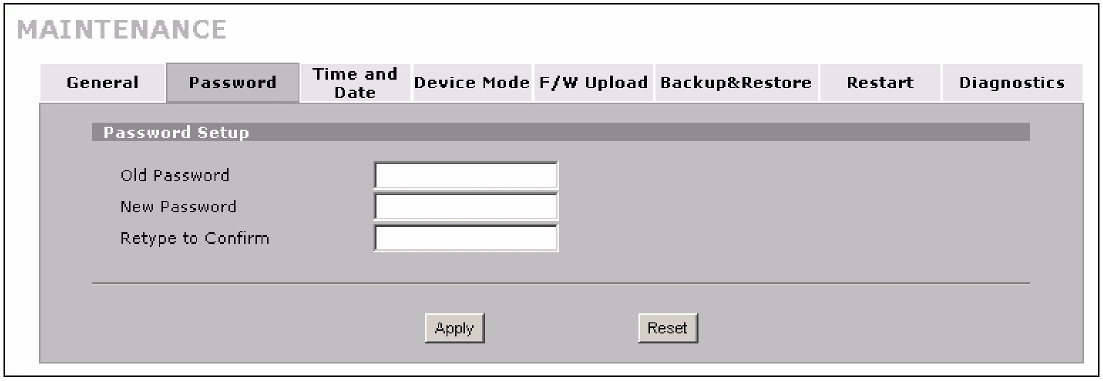
**Table 160** MAINTENANCE > General Setup

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| System Name | Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Domain Name | The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name), the domain name can be assigned from the ZyWALL via DHCP.<br>Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP.<br>The domain name entered by you is given priority over the ISP assigned domain name. |
| Administrator Inactivity Timer | Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 26.3 Configuring Password

Click **MAINTENANCE** > **Password** to open the following screen. Use this screen to change the ZyWALL's management password.

**Figure 280** MAINTENANCE > Password


MAINTENANCE
General
Password
Time and Date
Device Mode
F/W Upload
Backup&Restore
Restart
Diagnostics
Password Setup
Old Password
New Password
Retype to Confirm
Apply
Reset

The following table describes the labels in this screen.

**Table 161** MAINTENANCE > Password

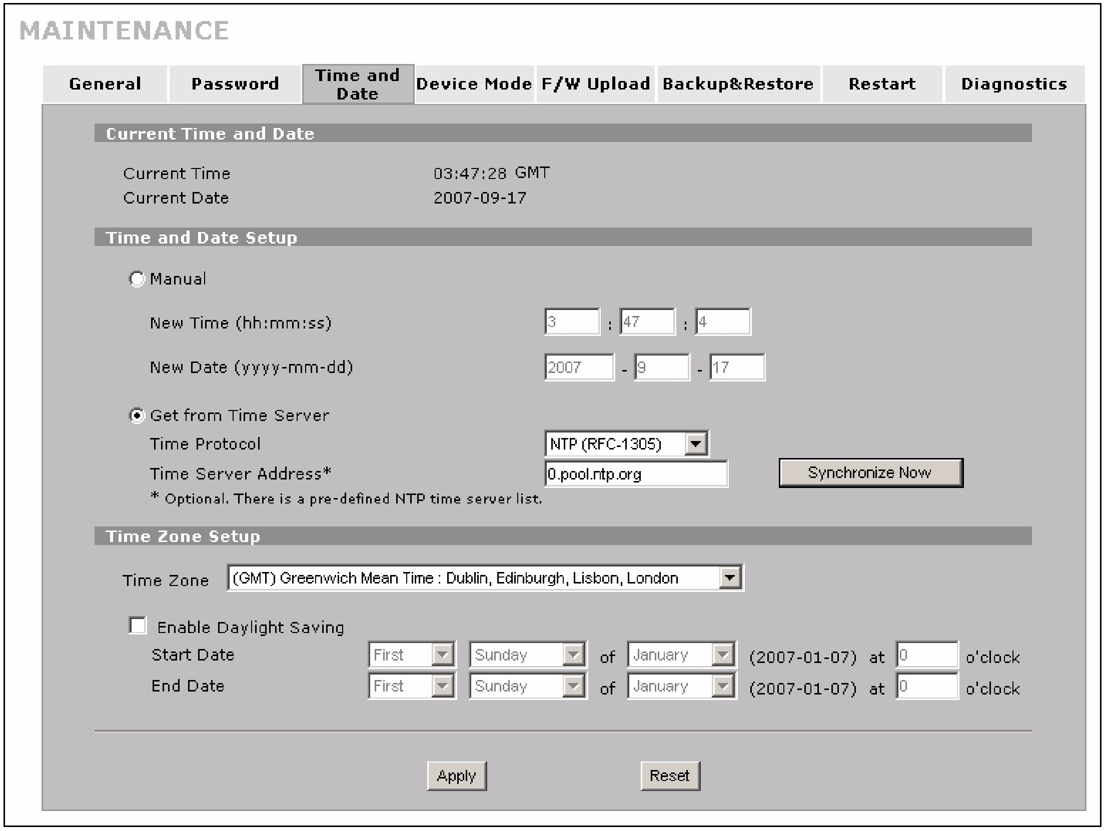
| LABEL | DESCRIPTION |
|---|---|
| Old Password | Type the default password or the existing password you use to access the system in this field. If you forget the password, you may have to use the hardware **RESET** button. This restores the default password of 1234. |
| New Password | Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. |
| Retype to Confirm | Type the new password again for confirmation. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 26.4 Time and Date

The ZyWALL's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL.

To change your ZyWALL's time and date, click **MAINTENANCE** > **Time and Date**. The screen appears as shown. Use this screen to configure the ZyWALL's time based on your local time zone.

**Figure 281** MAINTENANCE > Time and Date



Current Time and Date

Current Time 03:47:28 GMT
Current Date 2007-09-17

Time and Date Setup

○ Manual

New Time (hh:mm:ss) 3 : 47 : 4
New Date (yyyy-mm-dd) 2007 - 9 - 17

● Get from Time Server

Time Protocol NTP (RFC-1305)
Time Server Address* 0.pool.ntp.org
* Optional. There is a pre-defined NTP time server list.

Time Zone Setup

Time Zone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

☐ Enable Daylight Saving

Start Date First Sunday of January (2007-01-07) at 0 o'clock
End Date First Sunday of January (2007-01-07) at 0 o'clock

The following table describes the labels in this screen.

**Table 162** MAINTENANCE > Time and Date

| LABEL | DESCRIPTION |
|---|---|
| Current Time and Date | |
| Current Time | This field displays the ZyWALL's present time. |
| Current Date | This field displays the ZyWALL's present date. |
| Time and Date Setup | |
| Manual | Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it. |
| New Time (hh:mm:ss) | This field displays the last updated time from the time server or the last time configured manually.<br>When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**. |
| New Date (yyyy-mm-dd) | This field displays the last updated date from the time server or the last date configured manually.<br>When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**. |
| Get from Time Server | Select this radio button to have the ZyWALL get the time and date from the time server you specified below. |

**Table 162** MAINTENANCE > Time and Date (continued)

| LABEL | DESCRIPTION |
|---|---|
| Time Protocol | Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.<br>The main difference between them is the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>The default, **NTP (RFC 1305)**, is similar to **Time (RFC 868)**. |
| Time Server Address | Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information. |
| Synchronize Now | Click this button to have the ZyWALL get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (including the time server address). |
| Time Zone Setup | |
| Time Zone | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Enable Daylight Saving | Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.<br>Select this option if you use Daylight Saving Time. |
| Start Date | Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples:<br>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field.<br>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Date | Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples:<br>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field.<br>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 26.5 Pre-defined NTP Time Server Pools

When you turn on the ZyWALL for the first time, the date and time start at 2000-01-01 00:00:00. The ZyWALL then attempts to synchronize with an NTP time server from one of the 0.pool.ntp.org, 1.pool.ntp.org or 2.pool.ntp.org NTP time server pools. These are virtual clusters of time servers that use a round robin method to provide different NTP servers to clients.

The ZyWALL continues to use the NTP time server pools if you do not specify a time server or it cannot synchronize with the time server you specified.

The ZyWALL can use the NTP time server pools regardless of the time protocol you select.

When the ZyWALL uses the NTP time server pools, it randomly selects one pool and tries to synchronize with a server in it. If the synchronization fails, then the ZyWALL goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time server pools have been tried.

### 26.5.1 Resetting the Time

The ZyWALL resets time and date settings from the time server under the following circumstances.

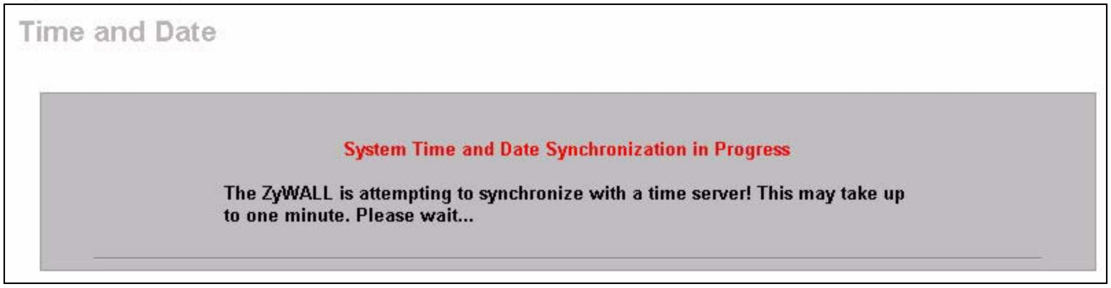
- When the ZyWALL starts up.
- When you click **Apply** or **Synchronize Now** in the **Time Setting** screen.
- 24-hour intervals after starting up.

### 26.5.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the predefined time server or the time server you specified in the **Time Server Address** field.

When the **System Time and Date Synchronization in Process** screen appears, wait up to one minute.

**Figure 282** Synchronization in Process

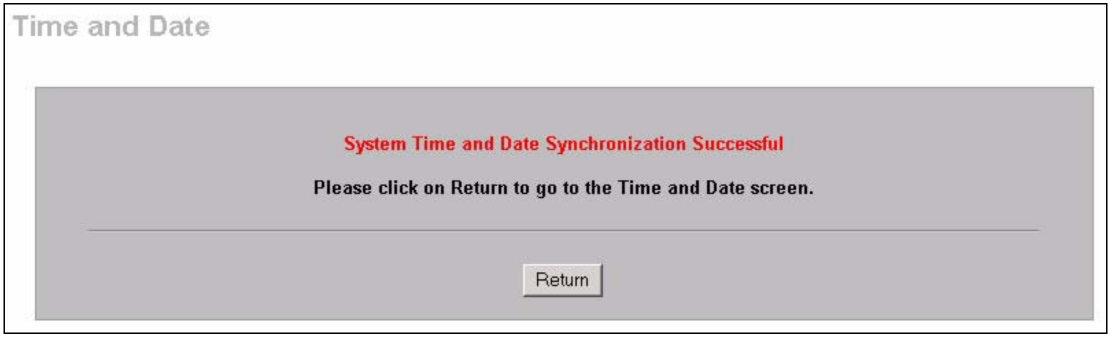


System Time and Date Synchronization in Progress

The ZyWALL is attempting to synchronize with a time server! This may take up to one minute. Please wait...

Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

**Figure 283** Synchronization is Successful



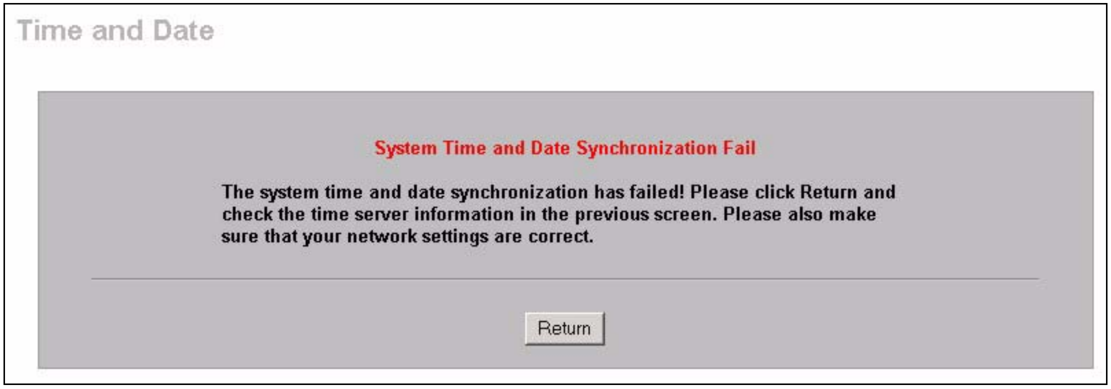
Time and Date

System Time and Date Synchronization Successful

Please click on Return to go to the Time and Date screen.

If the update was not successful, the following screen appears. Click **Return** to go back to the **Time and Date** screen.

**Figure 284** Synchronization Fail



Time and Date

System Time and Date Synchronization Fail

The system time and date synchronization has failed! Please click Return and check the time server information in the previous screen. Please also make sure that your network settings are correct.

## 26.6 Introduction To Transparent Bridging

A transparent bridge is invisible to the operation of a network in that it does not modify the frames it forwards. The bridge checks the source address of incoming frames on the port and learns MAC addresses to associate with that port. All future communications to that MAC address will only be sent on that port.

The bridge gradually builds a host MAC-address-to-port mapping table such as in the following example, during the learning process.

**Table 163** MAC-address-to-port Mapping Table

| HOST MAC ADDRESS | PORT |
|---|---|
| 00a0c5123456 | 3 |
| 00a0c5123478 (host A) | 1 |
| 00a0c512349a | 3 |
| 00a0c51234bc | 2 |
| 00a0c51234de | 4 |

For example, if a bridge receives a frame via port 1 from host A (MAC address 00a0c5123478), the bridge associates host A with port 1. When the bridge receives another frame on one of its ports with destination address 00a0c5123478, it forwards the frame directly through port 1 after checking the internal table.

The bridge takes one of these actions after it checks the destination address of an incoming frame with its internal table:

- If the table contains an association between the destination address and any of the bridge's ports aside from the one on which the frame was received, the frame is forwarded out the associated port.
- If no association is found, the frame is flooded to all ports except the inbound port. Broadcasts and multicasts also are flooded in this way.
- If the associated port is the same as the incoming port, then the frame is dropped (filtered).

## 26.7 Transparent Firewalls

A transparent firewall (also known as a transparent, in-line, shadow, stealth or bridging firewall) has the following advantages over “router firewalls”:

1. The use of a bridging firewall reduces configuration and deployment time because no networking configuration changes to your existing network (hosts, neighboring routers and the firewall itself) are needed. Just put it in-line with the network it is protecting. As it only moves frames between ports (after inspecting them), it is completely transparent.
2. Performance is improved as there's less processing overhead.
3. As a transparent bridge does not modify the frames it forwards, it is effectively “stealth” as it is invisible to attackers.

Bridging devices are most useful in complex environments that require a rapid or new firewall deployment. A transparent, bridging firewall can also be good for companies with several branch offices since the setups at these offices are often the same and it's likely that one design can be used for many of the networks. A bridging firewall could be configured at HQ, sent to the branches and then installed directly without additional configuration.

## 26.8 Configuring Device Mode (Router)

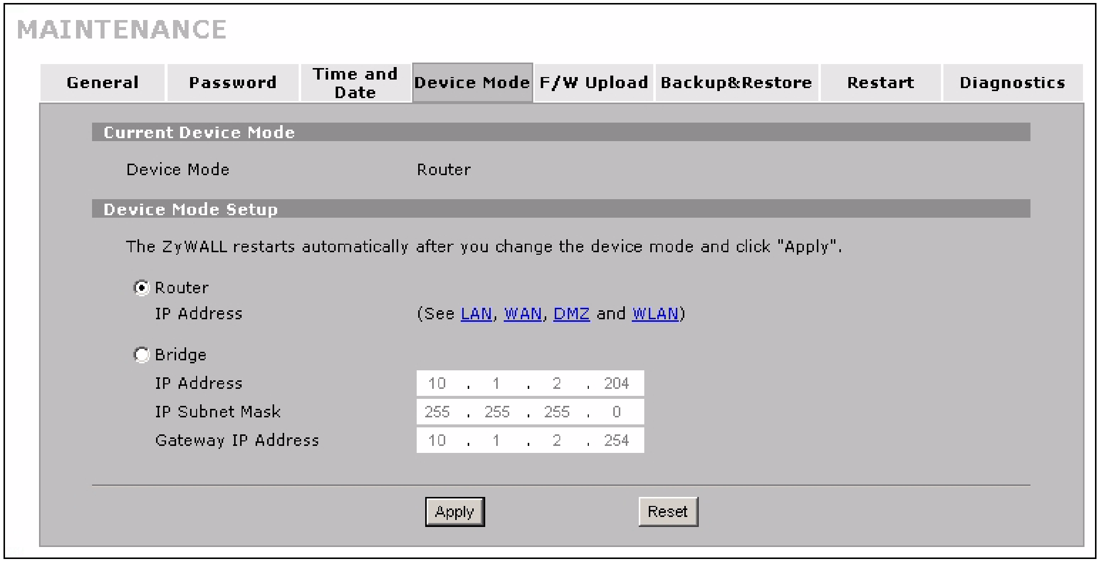
Click **MAINTENANCE** > **Device Mode** to open the following screen. Use this screen to configure your ZyWALL as a router or a bridge.

In router mode, the ZyWALL functions as a router. The ZyWALL routes traffic traveling between the ZyWALL's interfaces and filters and inspects packets.

In router mode, the ZyWALL can get an IP address from a DHCP server. It can also serve as a DHCP server to assign IP addresses to your local computers. The LAN, WAN, DMZ and WLAN interfaces all have different IP addresses. The ZyWALL also provides NAT, port forwarding, policy routing, and DNS in router mode. These features allow you to set up private network. See Table 5 on page 60 in the user’s guide for a detailed list of other features available in router mode.

The following applies when the ZyWALL is in router mode.

**Figure 285** MAINTENANCE > Device Mode (Router Mode)



Device Mode Router

The ZyWALL restarts automatically after you change the device mode and click "Apply".

● Router
IP Address (See LAN, WAN, DMZ and WLAN)

○ Bridge
IP Address 10 . 1 . 2 . 204
IP Subnet Mask 255 . 255 . 255 . 0
Gateway IP Address 10 . 1 . 2 . 254

The following table describes the labels in this screen.

**Table 164** MAINTENANCE > Device Mode (Router Mode)

| LABEL | DESCRIPTION |
|---|---|
| Current Device Mode | |
| Device Mode | This displays whether the ZyWALL is functioning as a router or a bridge. |
| Device Mode Setup | |
| Router | When the ZyWALL is in router mode, there is no need to select or clear this radio button. |
| IP Address | Click **LAN**, **WAN**, **DMZ** or **WLAN** to go to the **LAN**, **WAN**, **DMZ** or **WLAN** screen where you can view and/or change the corresponding settings. |
| Bridge | Select this radio button and configure the following fields, then click **Apply** to set the ZyWALL to bridge mode. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation. Use an IP address in the same subnet as the network to which you connect the ZyWALL. Make sure the IP address does not conflict with any other device on the network. |
| IP Subnet Mask | Enter the IP subnet mask of the ZyWALL. |
| Gateway IP Address | Enter the gateway IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. After you click **Apply**, please wait for one minute and use the IP address you configured in the **IP Address** field to access the ZyWALL again. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 26.9 Configuring Device Mode (Bridge)

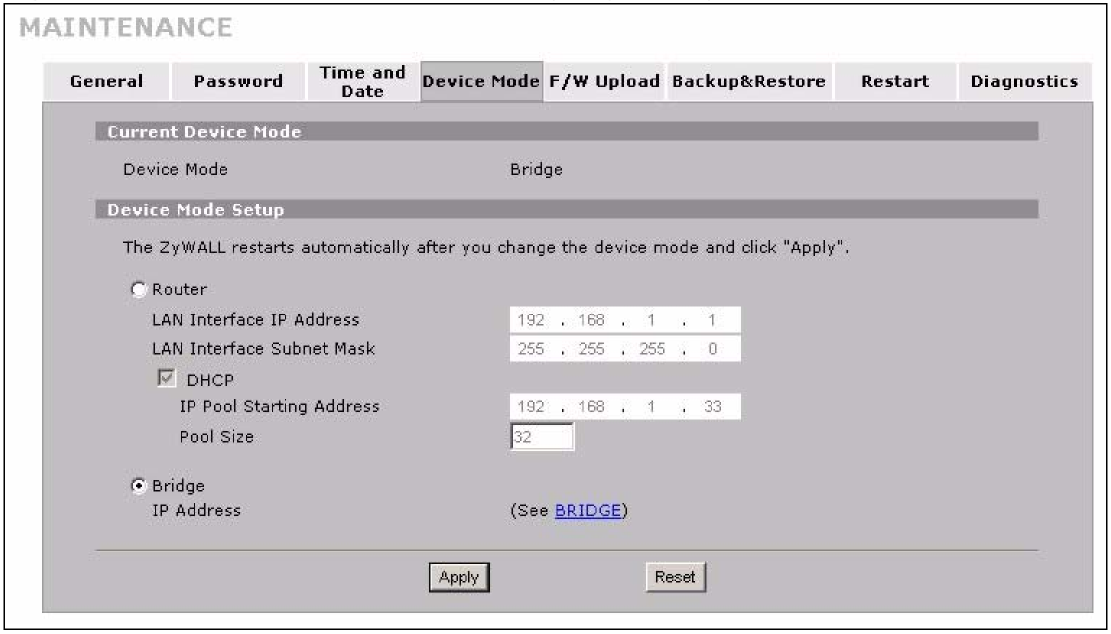
Click **MAINTENANCE** > **Device Mode** to open the following screen. Use this screen to configure your ZyWALL as a router or a bridge.

In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.

In bridge mode, the ZyWALL cannot get an IP address from a DHCP server. The LAN, WAN, DMZ and WLAN interfaces all have the same (static) IP address and subnet mask. You can configure the ZyWALL's IP address in order to access the ZyWALL for management. If you connect your computer directly to the ZyWALL, you also need to assign your computer a static IP address in the same subnet as the ZyWALL's IP address in order to access the ZyWALL.

You can use the firewall and VPN in bridge mode. See the user’s guide for a list of other features that are available in bridge mode.

**Figure 286** MAINTENANCE > Device Mode (Bridge Mode)



Device Mode: Bridge

The ZyWALL restarts automatically after you change the device mode and click "Apply".

○ Router
LAN Interface IP Address: 192 . 168 . 1 . 1
LAN Interface Subnet Mask: 255 . 255 . 255 . 0
☑ DHCP
IP Pool Starting Address: 192 . 168 . 1 . 33
Pool Size: 32

● Bridge
IP Address: (See BRIDGE)

The following table describes the labels in this screen.

**Table 165** MAINTENANCE > Device Mode (Bridge Mode)

| LABEL | DESCRIPTION |
|---|---|
| Current Device Mode | |
| Device Mode | This displays whether the ZyWALL is functioning as a router or a bridge. |
| Device Mode Setup | |
| Router | Select this radio button and click **Apply** to set the ZyWALL to router mode. |
| LAN Interface IP Address | Enter the IP address of your ZyWALL’ s LAN port in dotted decimal notation. 192.168.1.1 is the factory default. |
| LAN Interface Subnet Mask | Enter the IP subnet mask of the ZyWALL’s LAN port. |

**Table 165** MAINTENANCE > Device Mode (Bridge Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| DHCP | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the **DHCP** check box selected. Clear it to stop the ZyWALL from acting as a DHCP server. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the rest of the DHCP setup fields. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| Bridge | When the ZyWALL is in bridge mode, there is no need to select or clear this radio button. |
| IP Address | Click **Bridge** to go to the **Bridge** screen where you can view and/or change the bridge settings. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. After you click **Apply**, please wait for one minute and use the IP address you configured in the **LAN Interface IP Address** field to access the ZyWALL again. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

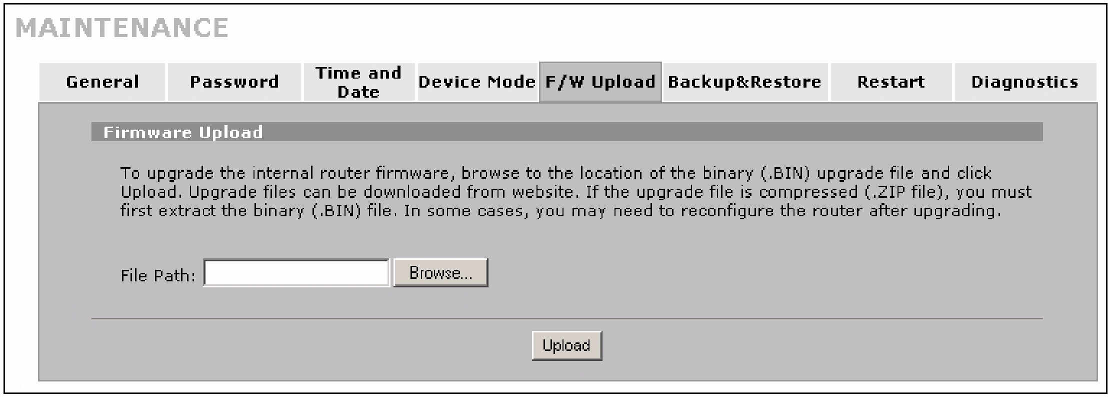
## 26.10 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "zywall.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section 41.5 on page 579 for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE** > **F/W UPLOAD**. Follow the instructions in this screen to upload firmware to your ZyWALL.

Only upload firmware for your specific model!

**Figure 287** MAINTENANCE > Firmware Upload



To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure the router after upgrading.

File Path:

The following table describes the labels in this screen.

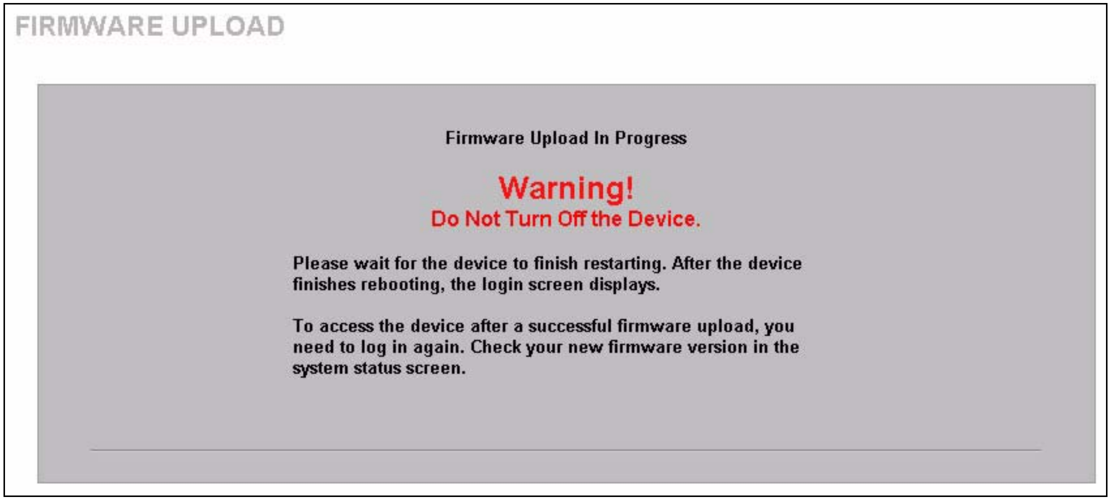
Table 166 MAINTENANCE > Firmware Upload

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |
| Browse... | Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Upload | Click **Upload** to begin the upload process. This process may take up to two minutes. |

Do not turn off the ZyWALL while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyWALL again.

Figure 288 Firmware Upload In Process



FIRMWARE UPLOAD

Firmware Upload In Progress

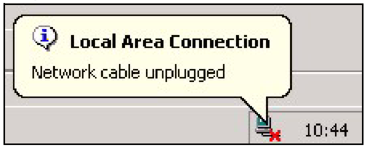
Warning!
Do Not Turn Off the Device.

Please wait for the device to finish restarting. After the device finishes rebooting, the login screen displays.

To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status screen.

The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 289 Network Temporarily Disconnected

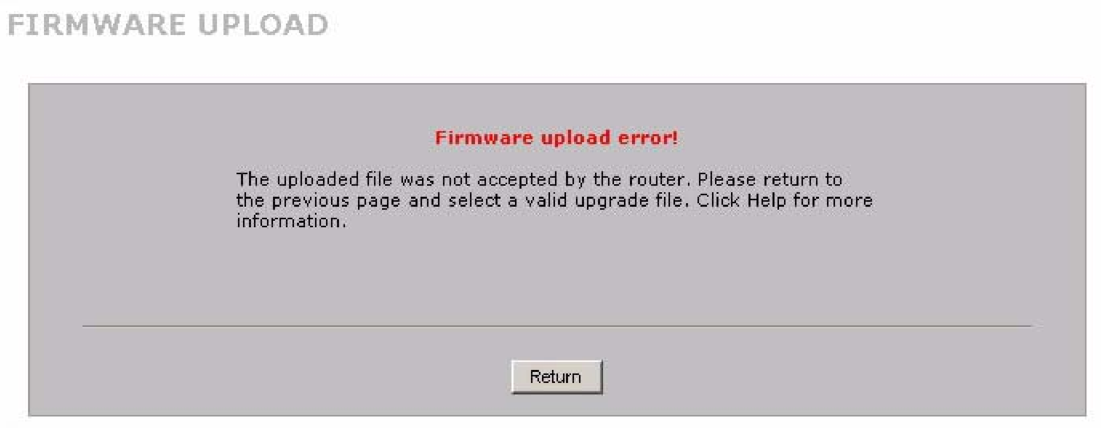


Local Area Connection
Network cable unplugged

After two minutes, log in again and check your new firmware version in the **HOME** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

**Figure 290** Firmware Upload Error


FIRMWARE UPLOAD
Return

Firmware upload error!

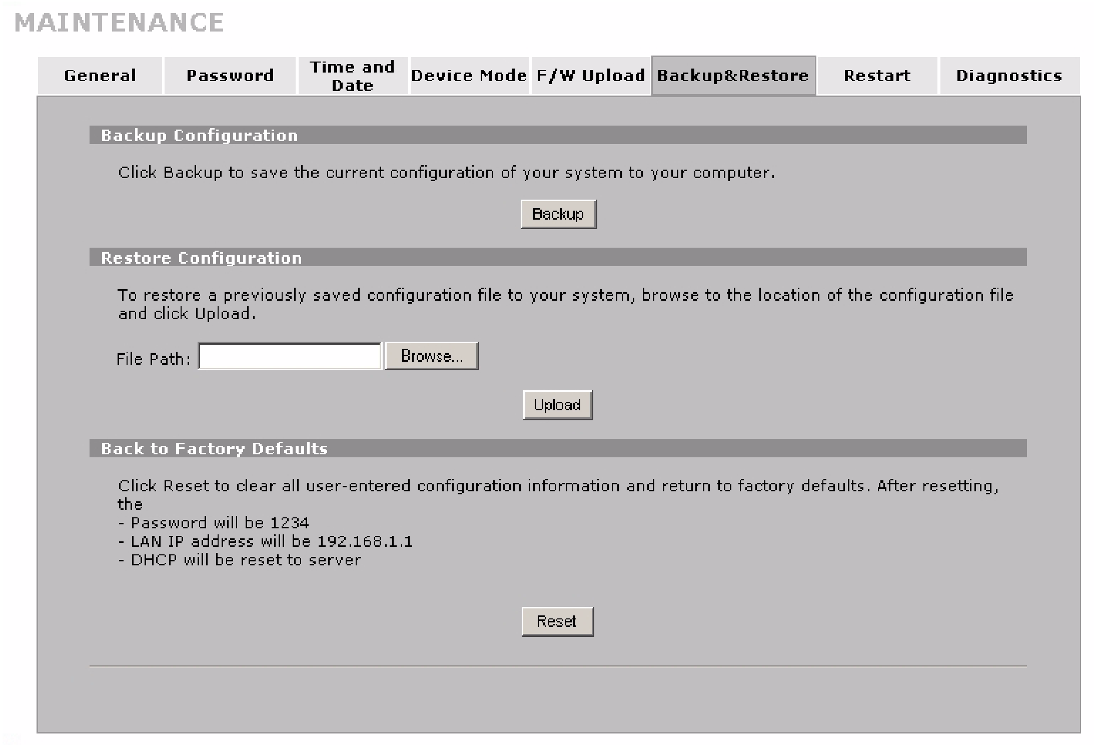
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.

## 26.11 Backup and Restore

See Section 41.5 on page 579 for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE** > **Backup & Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

**Figure 291** MAINTENANCE > Backup and Restore


MAINTENANCE
General
Password
Time and Date
Device Mode
F/W Upload
Backup&Restore
Restart
Diagnostics
Backup Configuration
Backup
Restore Configuration
File Path:
Browse...
Upload
Back to Factory Defaults
Reset

Click Backup to save the current configuration of your system to your computer.

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

## 26.11.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyWALL's current configuration to a file on your computer. Once your ZyWALL is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyWALL's current configuration to your computer.

## 26.11.2 Restore Configuration

Load a configuration file from your computer to your ZyWALL.

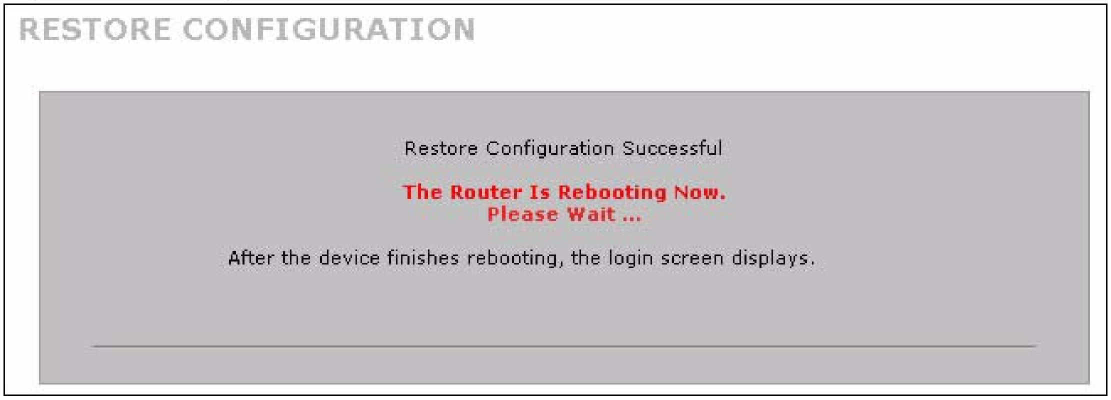
**Table 167** Restore Configuration

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |
| Browse... | Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them. |
| Upload | Click **Upload** to begin the upload process. |

Do not turn off the ZyWALL while configuration file upload is in progress.

After you see a "restore configuration successful" screen, you must then wait one minute before logging into the ZyWALL again.

**Figure 292** Configuration Upload Successful



RESTORE CONFIGURATION

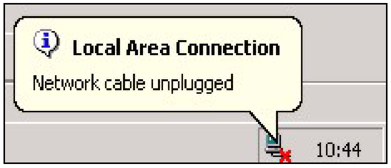
Restore Configuration Successful

The Router Is Rebooting Now.
Please Wait ...

After the device finishes rebooting, the login screen displays.

The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 293** Network Temporarily Disconnected

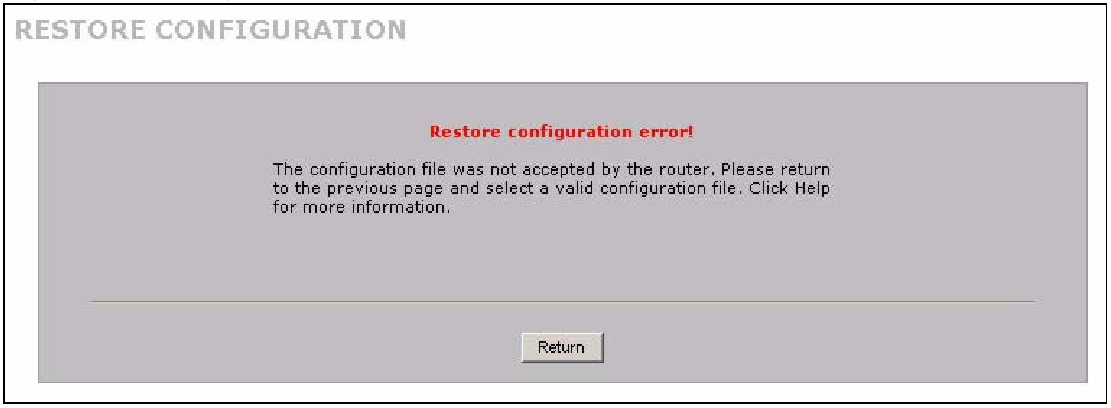


Local Area Connection
Network cable unplugged

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your Quick Start Guide for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

**Figure 294** Configuration Upload Error



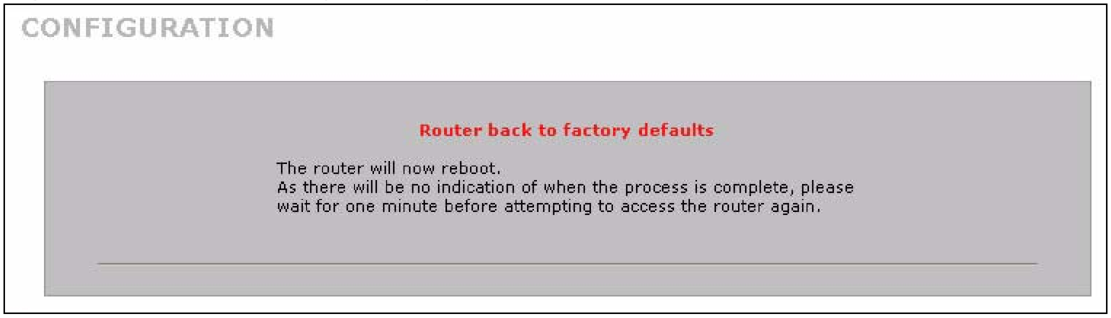
Restore configuration error!

The configuration file was not accepted by the router. Please return to the previous page and select a valid configuration file. Click Help for more information.

## 26.11.3 Back to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyWALL to its factory defaults as shown on the screen. The following warning screen appears.

**Figure 295** Reset Warning Message



Router back to factory defaults

The router will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the router again.

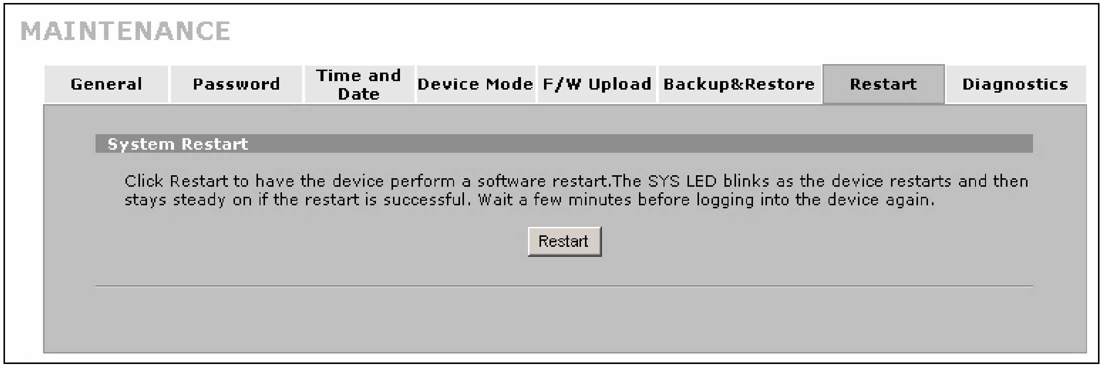
You can also press the hardware **RESET** button to reset the factory defaults of your ZyWALL. Refer to Section 2.3 on page 53 for more information on the **RESET** button.

# 26.12 Restart Screen

System restart allows you to reboot the ZyWALL without turning the power off.

Click **MAINTENANCE** > **Restart**. Click **Restart** to have the ZyWALL reboot. Restart is different to reset; (see Section 26.11.3 on page 461) reset returns the device to its default configuration.

**Figure 296** MAINTENANCE > Restart


MAINTENANCE
General
Password
Time and Date
Device Mode
F/W Upload
Backup&Restore
Restart
Diagnostics
System Restart
Restart

Click Restart to have the device perform a software restart.The SYS LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a few minutes before logging into the device again.

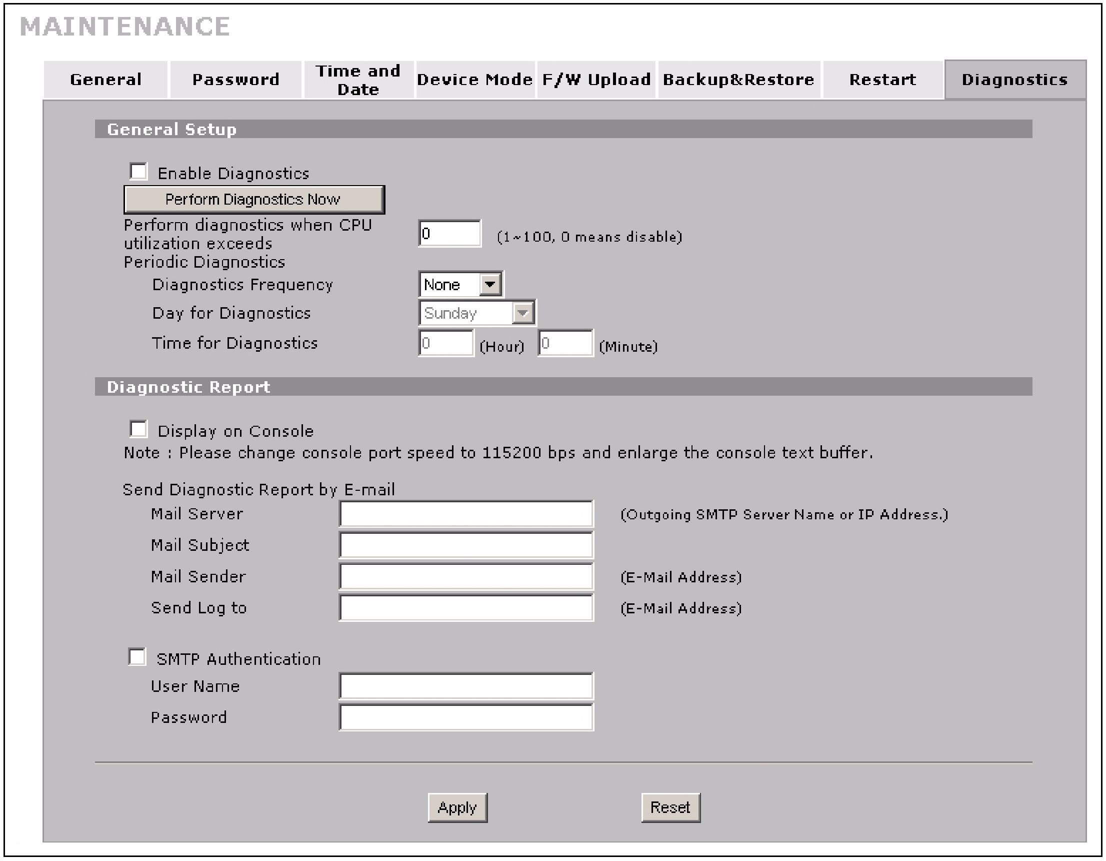
## 26.13 Diagnostics

Use the **Diagnostics** screen to have the ZyWALL generate and send diagnostic files by e-mail and/or the console port. The diagnostics files contain the ZyWALL's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

Click **MAINTENANCE** > **Diagnostics** to open the following screen.

The ZyWALL sends only one diagnosis mail within five minutes (unless you click **Perform Diagnostics Now**).

**Figure 297** MAINTENANCE > Diagnostics



☐ Enable Diagnostics

Perform diagnostics when CPU utilization exceeds: 0 (1~100, 0 means disable)

Periodic Diagnostics

Diagnostics Frequency: None

Day for Diagnostics: Sunday

Time for Diagnostics: 0 (Hour) 0 (Minute)

☐ Display on Console

Note : Please change console port speed to 115200 bps and enlarge the console text buffer.

Send Diagnostic Report by E-mail

Mail Server: (Outgoing SMTP Server Name or IP Address.)

Mail Subject:

Mail Sender: (E-Mail Address)

Send Log to: (E-Mail Address)

☐ SMTP Authentication

User Name:

Password:

The following table describes the labels in this screen.

**Table 168** MAINTENANCE > Diagnostics

| LABEL | DESCRIPTION |
|---|---|
| Enable Diagnostics | Select this option to turn on the diagnostics feature. |
| Perform Diagnostics Now | Click this button to generate and send a diagnostic file immediately, instead of based on a time period or CPU usage level. |
| Perform diagnostics when CPU utilization exceeds | Set the ZyWALL to generate and send a diagnostic file every time the CPU usage exceeds the specified percent for more than 60 seconds. Enter 0 to have the ZyWALL not generate and send diagnostic files based on CPU usage going over a specific level. |
| Periodic Diagnostics | Use these fields to set the ZyWALL to generate and send diagnostic files at regular intervals.<br>Even if you enable both CPU utilization-based and periodic diagnosis, the ZyWALL only sends one diagnostic file within five minutes (unless you click **Perform Diagnostics Now**). |
| Diagnostics Frequency | Set how often the ZyWALL generates and sends diagnostic files.<br>**Hourly**<br>**Daily**<br>**Weekly**<br>**None**.<br>If you select **Daily** or **Weekly**, specify a time of day for the ZyWALL to generate and send diagnostic files. If you select **Weekly**, then also specify which day of the week. Select **None** to have the ZyWALL not generate and send diagnostic files based on a time period. |

**Table 168** MAINTENANCE > Diagnostics (continued)

| LABEL | DESCRIPTION |
|---|---|
| Day for Diagnostics | Use the drop down list box to select which day of the week to generate and send diagnostic files. |
| Time for Diagnostics | Enter the time of day in 24-hour format (for example 23:00 equals 11:00 pm) to generate and send diagnostic files. |
| Display on Console | Select this option to have the ZyWALL send diagnostic information through the console port. To receive the information through the console port, you still need to configure the mail settings and open a terminal emulation program on the computer connected to the console port.<br>To handle the size of the diagnostic file, change your console port speed to 115200 bps (on both the ZyWALL and your terminal emulation program) and enlarge the console text buffer. |
| Send Diagnostic Report by E-mail | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail address specified in the **Mail Sender** field. If this field is left blank, diagnostic files will not be sent via e-mail. |
| Mail Subject | Type a title that you want to be in the subject line of the diagnostic e-mail message that the ZyWALL sends. |
| Mail Sender | Enter the e-mail address that you want to be in the from/sender line of the diagnostic e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well. |
| Send Log to | Diagnostic files are sent to the e-mail address specified in this field. If this field is left blank, diagnostic files will not be sent via e-mail. |
| SMTP Authentication | SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.<br>Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the diagnostic files. |
| User Name | Enter the user name (up to 31 characters) (usually the user name of a mail account you specified in the **Mail Sender** field). |
| Password | Enter the password associated with the user name above. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# PART VI

# SMT

Introducing the SMT (467)
SMT Menu 1 - General Setup (475)
WAN and Dial Backup Setup (481)
LAN Setup (491)
Internet Access (497)
DMZ Setup (501)
Remote Node Setup (509)
IP Static Route Setup (519)
Network Address Translation (NAT) (521)
Introducing the ZyWALL Firewall (539)
Filter Configuration (541)
SNMP Configuration (557)
System Information & Diagnosis (559)
Firmware and Configuration File Maintenance (571)
System Maintenance Menus 8 to 10 (587)
Remote Management (595)
Call Scheduling (599)

# 27

# Introducing the SMT

This chapter explains how to access the System Management Terminal and gives an overview of its menus.

## 27.1 Introduction to the SMT

The ZyWALL's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

## 27.2 Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the Quick Start Guide.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

### 27.2.1 Initial Screen

When you turn on your ZyWALL, it performs several internal tests as well as line initialization.

After the tests, the ZyWALL asks you to press [ENTER] to continue, as shown next.

**Figure 298** Initial Screen

```
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.

initialize ch =0, ethernet address: 00:A0:C5:01:23:45
initialize ch =1, ethernet address: 00:A0:C5:01:23:46
initialize ch =2, ethernet address: 00:A0:C5:01:23:47
initialize ch =3, ethernet address: 00:A0:C5:01:23:48
initialize ch =4, ethernet address: 00:00:00:00:00:00
AUX port init . done
Modem init . inactive

Press ENTER to continue...
```

## 27.2.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below.

For your first login, enter the default password “1234”. As you type the password, the screen displays an “X” for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your ZyWALL will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

**Figure 299** Password Screen

```
Enter Password : XXXX
```

# 27.3 Navigating the SMT Interface

The SMT is an interface that you use to configure your ZyWALL.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

**Table 169** Main Menu Commands

| OPERATION | KEYSTROKES | DESCRIPTION |
|---|---|---|
| Move down to another menu | [ENTER] | To move forward to a submenu, type in the number of the desired submenu and press [ENTER]. |
| Move up to a previous menu | [ESC] | Press the [ESC] key to move back to the previous menu. |
| Move to a “hidden” menu | Press [SPACE BAR] to change No to Yes then press [ENTER]. | Fields beginning with “Edit” lead to hidden menus and have a default setting of No. Press [SPACE BAR] to change No to Yes, and then press [ENTER] to go to a “hidden” menu. |

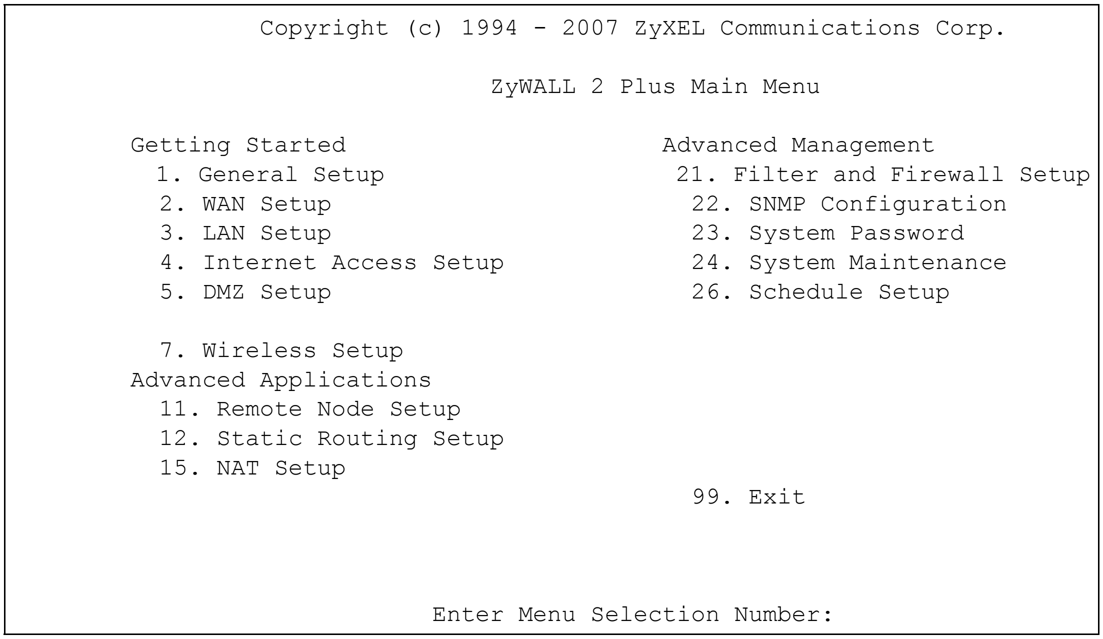
**Table 169** Main Menu Commands

| OPERATION | KEYSTROKES | DESCRIPTION |
|---|---|---|
| Move the cursor | [ENTER] or [UP]/ [DOWN] arrow keys | Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.<br>When you are at the top of a menu, press the [UP] arrow key to move to the bottom of a menu. |
| Entering information | Fill in, or press [SPACE BAR], then press [ENTER] to select from choices. | You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR]. |
| Required fields | <? > | All fields with the symbol <?> must be filled in order be able to save the new configuration. |
| N/A fields | <N/A> | Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable. |
| Save your configuration | [ENTER] | Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu.<br>Make sure you save your settings in each screen that you configure. |
| Exit the SMT | Type 99, then press [ENTER]. | Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface. |

## 27.3.1 Main Menu

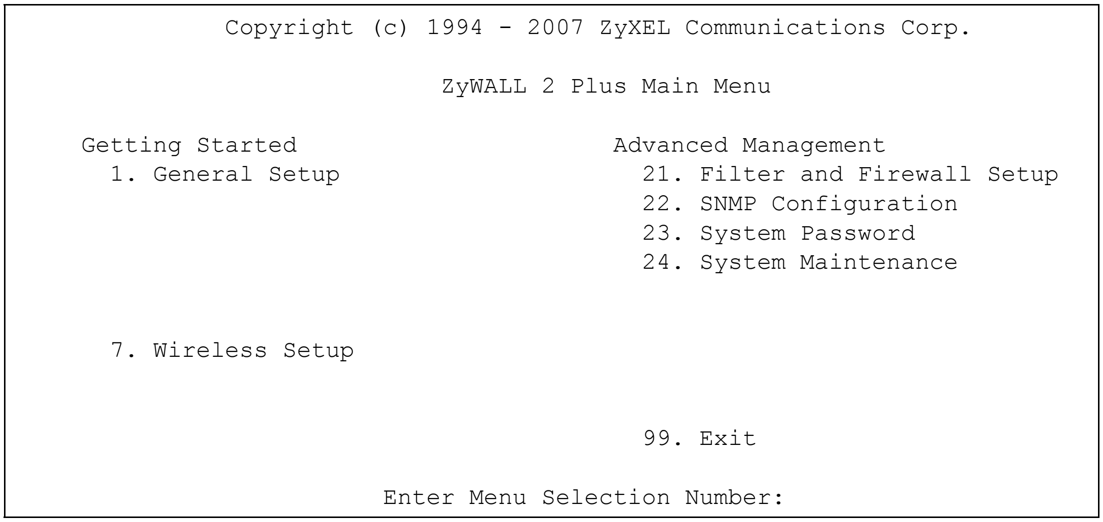
After you enter the password, the SMT displays the **ZyWALL Main Menu**, as shown next.

**Figure 300** Main Menu (Router Mode)



```
                  Copyright (c) 1994 - 2007 ZyXEL Communications Corp.

                                  ZyWALL 2 Plus Main Menu

         Getting Started                       Advanced Management
           1. General Setup                     21. Filter and Firewall Setup
           2. WAN Setup                          22. SNMP Configuration
           3. LAN Setup                          23. System Password
           4. Internet Access Setup              24. System Maintenance
           5. DMZ Setup                          26. Schedule Setup

           7. Wireless Setup
         Advanced Applications
           11. Remote Node Setup
           12. Static Routing Setup
           15. NAT Setup
                                                 99. Exit



                              Enter Menu Selection Number:
```

**Figure 301** Main Menu (Bridge Mode)



```
               Copyright (c) 1994 - 2007 ZyXEL Communications Corp.

                              ZyWALL 2 Plus Main Menu

     Getting Started                      Advanced Management
       1. General Setup                     21. Filter and Firewall Setup
                                            22. SNMP Configuration
                                            23. System Password
                                            24. System Maintenance



       7. Wireless Setup



                                            99. Exit

                          Enter Menu Selection Number:
```

The following table describes the fields in this menu.

**Table 170** Main Menu Summary

| NO. | MENU TITLE | FUNCTION |
|---|---|---|
| 1 | General Setup | Use this menu to set up device mode, dynamic DNS and administrative information. |
| 2 | WAN Setup | Use this menu to clone a MAC address from a computer on your LAN and configure the backup WAN dial-up connection. |
| 3 | LAN Setup | Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings. |
| 4 | Internet Access Setup | Configure your Internet access setup (Internet address, gateway, login, etc.) with this menu. |
| 5 | DMZ Setup | Use this menu to apply DMZ filters, and configure DHCP and TCP/IP settings for the DMZ port. |
| 7 | Wireless Setup | Use this menu to configure WLAN DHCP and TCP/IP settings for the wireless LAN interface. |
| 11 | Remote Node Setup | Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters. |
| 12 | Static Routing Setup | Configure IP static routes in this menu. |
| 15 | NAT Setup | Use this menu to configure Network Address Translation. |
| 21 | Filter and Firewall Setup | Configure filters and activate/deactivate the firewall. |
| 22 | SNMP Configuration | Use this menu to configure SNMP-related parameters. |
| 23 | System Password | Change your password in this menu (recommended). |
| 24 | System Maintenance | From displaying system status to uploading firmware, this menu provides comprehensive system maintenance. |
| 26 | Schedule Setup | Use this menu to schedule outgoing calls. |
| 99 | Exit | Use this menu to exit (necessary for remote configuration). |

## 27.3.2 SMT Menus Overview

The following table gives you an overview of your ZyWALL's various SMT menus.

**Table 171** SMT Menus Overview

| MENUS | SUB MENUS | | |
|---|---|---|---|
| 1 General Setup | 1.1 Configure Dynamic DNS | 1.1.1 DDNS Host Summary | 1.1.1 DDNS Edit Host |
| 2 WAN Setup | 2.1 Advanced WAN Setup | | |
| 3 LAN Setup | 3.1 LAN Port Filter Setup | | |
| | 3.2 TCP/IP and DHCP Ethernet Setup | 3.2.1 IP Alias Setup | |
| 4 Internet Access Setup | | | |
| 5 DMZ Setup | 5.1 DMZ Port Filter Setup | | |
| | 5.2 TCP/IP and DHCP Ethernet Setup | 5.2.1 IP Alias Setup | |
| 7 Wireless Setup | 7.2 TCP/IP and DHCP Ethernet Setup | 7.2.1 IP Alias Setup | |
| 11 Remote Node Setup | 11.1 Remote Node Profile | 11.1.2 Remote Node Network Layer Options | |
| | | 11.1.4 Remote Node Filter | |
| | | 11.1.5 Traffic Redirect Setup | |
| | 11.2 Remote Node Profile (Backup ISP) | 11.2.2 Remote Node Network Layer Options | |
| | | 11.2.3 Remote Node Script | |
| | | 11.2.4 Remote Node Filter | |
| 12 Static Routing Setup | 12.1 Edit IP Static Route | | |
| 15 NAT Setup | 15.1 Address Mapping Sets | 15.1.x Address Mapping Rules | 15.1.x.x Address Mapping Rule |
| | 15.2 Port Forwarding Setup | 15.2.x NAT Server Setup | 15.2.x.x - NAT Server Configuration |
| | 15.3 Trigger Port Setup | | |
| 21 Filter and Firewall Setup | 21.1 Filter Setup | 21.1.x Filter Rules Summary | 21.1.x.x Generic Filter Rule |
| | | | 21.1.x.x TCP/IP Filter Rule |
| | 21.2 Firewall Setup | | |
| 22 SNMP Configuration | | | |
| 23 System Password | | | |

**Table 171** SMT Menus Overview (continued)

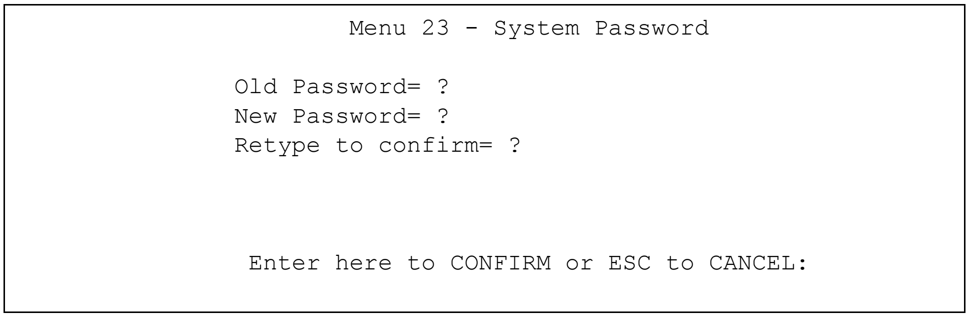
| MENUS | SUB MENUS | | |
|---|---|---|---|
| 24 System Maintenance | 24.1 System Status | | |
| | 24.2 System Information and Console Port Speed | 24.2.1 System Information | |
| | | 24.2.2 Console Port Speed | |
| | 24.3 Log and Trace | 24.3.1 View Error Log | |
| | | 24.3.2 Syslog Logging | |
| | | 24.3.4 Call-Triggering Packet | |
| | 24.4 Diagnostic | | |
| | 24.5 Backup Configuration | | |
| | 24.6 Restore Configuration | | |
| | 24.7 Upload Firmware | 24.7.1 Upload System Firmware | |
| | | 24.7.2 Upload System Configuration File | |
| | 24.8 Command Interpreter Mode | | |
| | 24.9 Call Control | 24.9.1 Budget Management | |
| | | 24.9.2 Call History | |
| | 24.10 Time and Date Setting | | |
| | 24.11 Remote Management Setup | | |
| 26 Schedule Setup | 26.1 Schedule Set Setup | | |

## 27.4 Changing the System Password

Change the system password by following the steps shown next.

1 Enter 23 in the main menu to open **Menu 23 - System Password** as shown next.

**Figure 302** Menu 23: System Password



```
                        Menu 23 - System Password

                Old Password= ?
                New Password= ?
                Retype to confirm= ?



                 Enter here to CONFIRM or ESC to CANCEL:
```

2 Type your existing password and press [ENTER].

3 Type your new system password and press [ENTER].

4 Re-type your new system password for confirmation and press [ENTER].

Note that as you type a password, the screen displays an “x” for each character you type.

## 27.5 Resetting the ZyWALL

See Section 2.3 on page 53 for directions on resetting the ZyWALL.

# 28

# SMT Menu 1 - General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

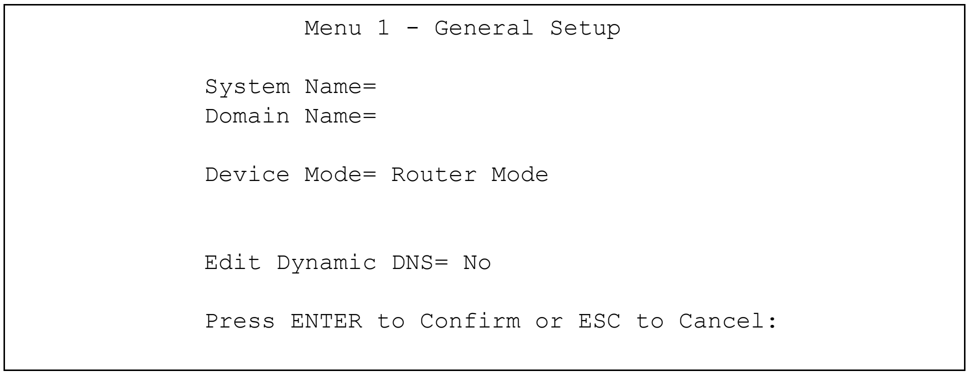
## 28.1 Introduction to General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

## 28.2 Configuring General Setup

1. Enter 1 in the main menu to open **Menu 1 - General Setup**.
2. The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.

**Figure 303** Menu 1: General Setup (Router Mode)



```
                     Menu 1 - General Setup

              System Name=
              Domain Name=

              Device Mode= Router Mode


              Edit Dynamic DNS= No

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

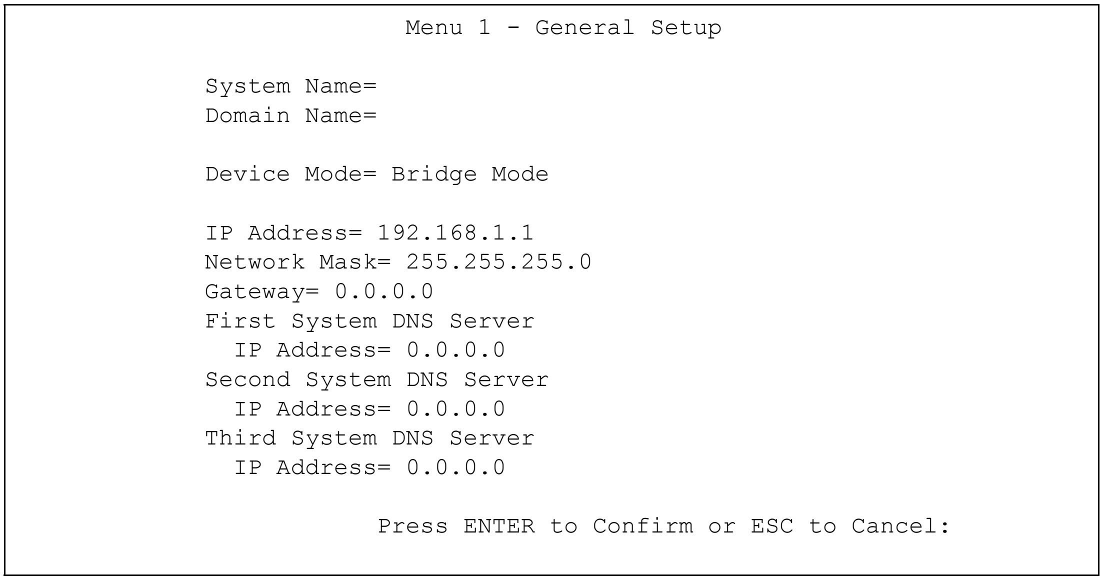
**Table 172** Menu 1: General Setup (Router Mode)

| FIELD | DESCRIPTION |
|---|---|
| System Name | Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Domain Name | Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router.<br>The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER]. |

**Table 172** Menu 1: General Setup (Router Mode) (continued)

| FIELD | DESCRIPTION |
|---|---|
| Device Mode | Press [SPACE BAR] and then [ENTER] to select **Router Mode**. |
| Edit Dynamic DNS | Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

**Figure 304** Menu 1: General Setup (Bridge Mode)



```
                            Menu 1 - General Setup

              System Name=
              Domain Name=

              Device Mode= Bridge Mode

              IP Address= 192.168.1.1
              Network Mask= 255.255.255.0
              Gateway= 0.0.0.0
              First System DNS Server
                IP Address= 0.0.0.0
              Second System DNS Server
                IP Address= 0.0.0.0
              Third System DNS Server
                IP Address= 0.0.0.0

                          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields not previously discussed (see Table 172 on page 475).

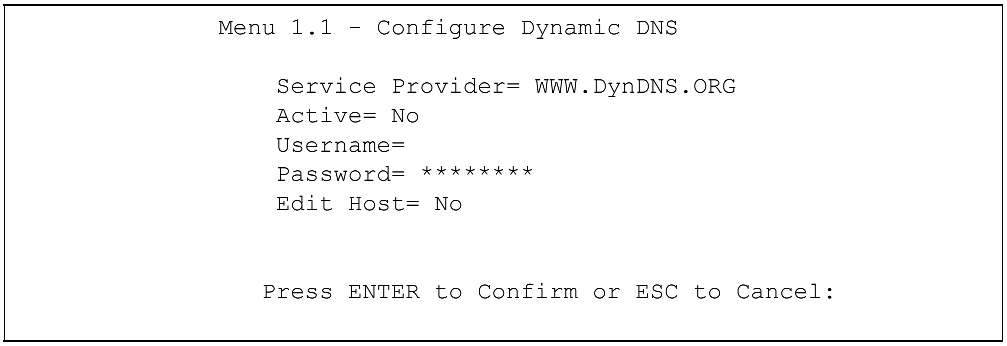
**Table 173** Menu 1: General Setup (Bridge Mode)

| FIELD | DESCRIPTION |
|---|---|
| Device Mode | Press [SPACE BAR] and then [ENTER] to select **Bridge Mode**. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation. |
| Network Mask | Enter the subnet mask of your ZyWALL. |
| Gateway | Enter the gateway IP address. |
| First System DNS Server<br>Second System DNS Server<br>Third System DNS Server | Enter the DNS server's IP address(es) in the **IP Address** field(s) if you have the IP address(es) of the DNS server(s). |

## 28.2.1 Configuring Dynamic DNS

To configure Dynamic DNS, set the ZyWALL to router mode in menu 1 or in the **MAINTENANCE Device Mode** screen and go to **Menu 1 - General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS** (shown next).

**Figure 305** Menu 1.1: Configure Dynamic DNS



```
              Menu 1.1 - Configure Dynamic DNS

                  Service Provider= WWW.DynDNS.ORG
                  Active= No
                  Username=
                  Password= ********
                  Edit Host= No


                 Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table to configure Dynamic DNS parameters.

**Table 174** Menu 1.1: Configure Dynamic DNS

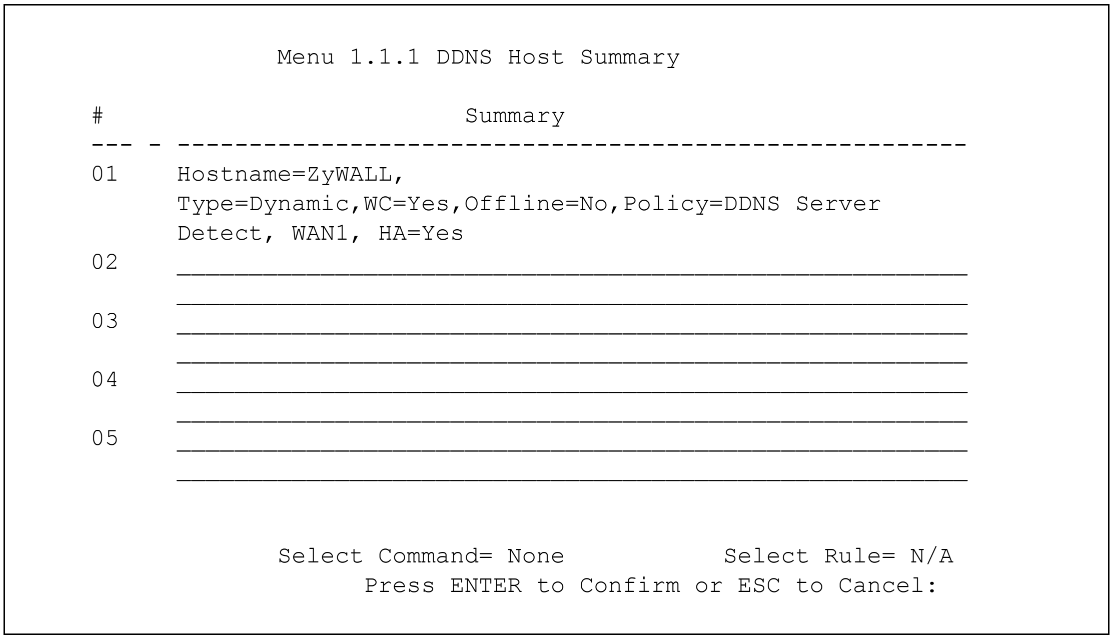
| FIELD | DESCRIPTION |
|---|---|
| Service Provider | This is the name of your Dynamic DNS service provider. |
| Active | Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active. |
| Username | Enter your user name. |
| Password | Enter the password assigned to you. |
| Edit Host | Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to configure a DDNS host. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

### 28.2.1.1 Editing DDNS Host

To configure a DDNS host, follow the procedure below.

1. Configure your ZyWALL as a router in menu 1 or the **MAINTENANCE Device Mode** screen.
2. Enter 1 in the main menu to open **Menu 1 - General Setup**.
3. Press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS**.
4. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Edit Host** field. Press [ENTER] to display **Menu 1.1.1 - DDNS Host Summary**.

**Figure 306** Menu 1.1.1: DDNS Host Summary



```
                 Menu 1.1.1 DDNS Host Summary

     #                        Summary
     --- - -------------------------------------------------------
     01    Hostname=ZyWALL,
           Type=Dynamic,WC=Yes,Offline=No,Policy=DDNS Server
           Detect, WAN1, HA=Yes
     02    _______________________________________________________
           _______________________________________________________
     03    _______________________________________________________
           _______________________________________________________
     04    _______________________________________________________
           _______________________________________________________
     05    _______________________________________________________
           _______________________________________________________


                  Select Command= None           Select Rule= N/A
                        Press ENTER to Confirm or ESC to Cancel:
```

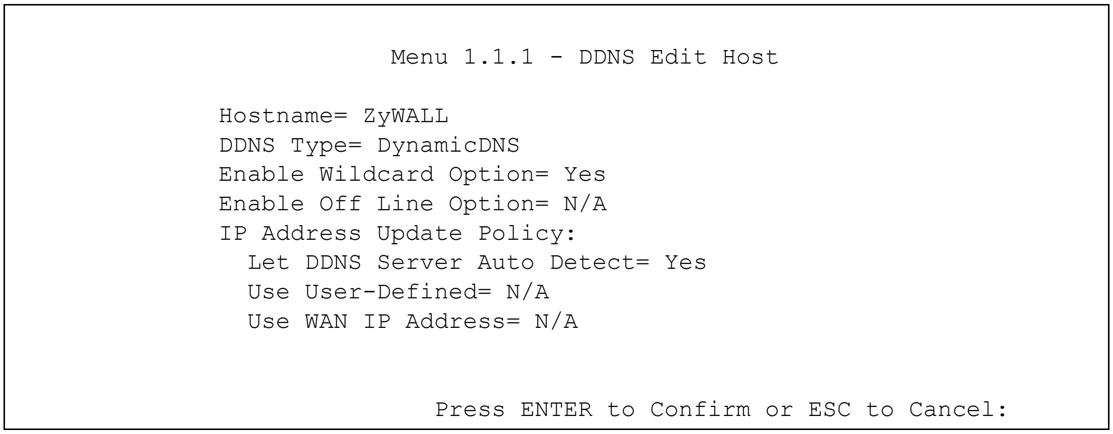
The following table describes the fields in this screen.

**Table 175** Menu 1.1.1: DDNS Host Summary

| FIELD | DESCRIPTION |
|---|---|
| # | This is the DDNS host index number. |
| Summary | This displays the details about the DDNS host. |
| Select Command | Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a DDNS host in the next field when you choose the **Edit** or **Delete** commands.<br>Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt.<br>Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a DDNS host, first make sure you are on the correct page. When a rule is deleted, subsequent rules do not move up in the page list.<br>Select **Next Page** or **Previous Page** to view the next or previous page of DDNS hosts (respectively). |
| Select Rule | Type the DDNS host index number you wish to edit or delete and then press [ENTER]. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

5 Select **Edit** in the **Select Command** field; type the index number of the DDNS host you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 1.1.1 - DDNS Edit Host** (see the next figure).

**Figure 307** Menu 1.1.1: DDNS Edit Host



```
                           Menu 1.1.1 - DDNS Edit Host

               Hostname= ZyWALL
               DDNS Type= DynamicDNS
               Enable Wildcard Option= Yes
               Enable Off Line Option= N/A
               IP Address Update Policy:
                 Let DDNS Server Auto Detect= Yes
                 Use User-Defined= N/A
                 Use WAN IP Address= N/A


                              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 176** Menu 1.1.1: DDNS Edit Host

| FIELD | DESCRIPTION |
|---|---|
| Host Name | Enter your host name in this field. |
| DDNS Type | Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have the Dynamic DNS service.<br>Select **StaticDNS** if you have the Static DNS service.<br>Select **CustomDNS** if you have the Custom DNS service. |
| Enable Wildcard Option | Your ZyWALL supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. This field is **N/A** when you choose DDNS client as your service provider. |
| Enable Off Line Option | This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, http://www.dyndns.org/ traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details). |
| IP Address Update Policy: | You can select **Yes** in either the **Let DDNS Server Auto Detect** field (recommended) or the **Use User-Defined** field, but not both.<br>With the **Let DDNS Server Auto Detect** and **Use User-Defined** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the ZyWALL's WAN IP address.<br>DDNS does not work with a private IP address. When both fields are set to **No**, the ZyWALL must have a public WAN IP address in order for DDNS to work. |
| Let DDNS Server Auto Detect | Only select this option when there are one or more **NAT** routers between the ZyWALL and the DDNS server. Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.<br>Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server. |
| Use User-Defined | Press [SPACE BAR] to select **Yes** and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below.<br>Only select **Yes** if the ZyWALL uses or is behind a static public IP address. |

**Table 176** Menu 1.1.1: DDNS Edit Host (continued)

| FIELD | DESCRIPTION |
|---|---|
| Use WAN IP Address | Enter the static public IP address if you select **Yes** in the **Use User-Defined** field. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

# 29

# WAN and Dial Backup Setup

This chapter describes how to configure the WAN using menu 2 and dial-backup using menus 2.1 and 11.1.

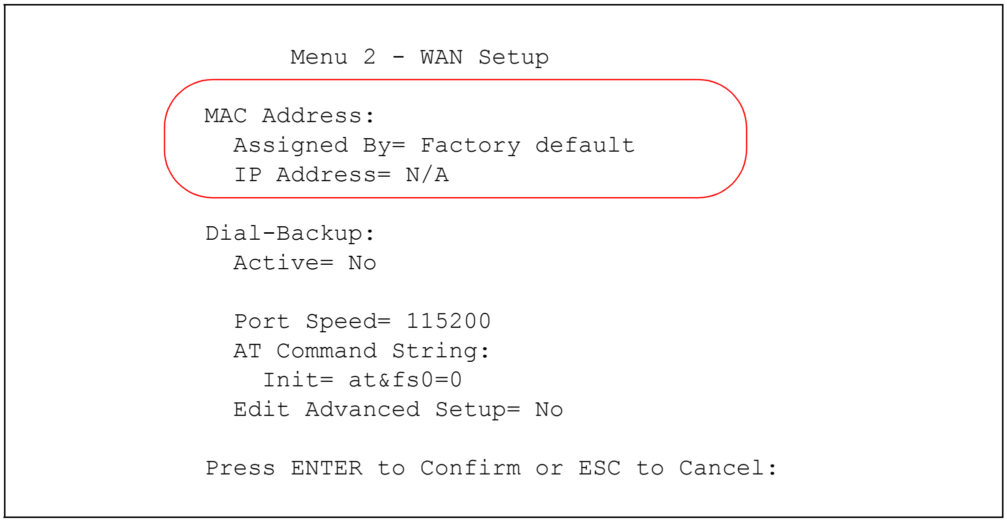
## 29.1 Introduction to WAN and Dial Backup Setup

This chapter explains how to configure settings for your WAN port and how to configure the ZyWALL for a dial backup connection.

## 29.2 WAN Setup

From the main menu, enter 2 to open menu 2.

**Figure 308** MAC Address Cloning in WAN Setup



```
                    Menu 2 - WAN Setup

              MAC Address:
                Assigned By= Factory default
                IP Address= N/A

              Dial-Backup:
                Active= No

                Port Speed= 115200
                AT Command String:
                  Init= at&fs0=0
                Edit Advanced Setup= No

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 177** MAC Address Cloning in WAN Setup

| FIELD | DESCRIPTION |
|---|---|
| MAC Address | |
| Assigned By | Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP address attached on LAN** to use the MAC Address of that computer whose IP you give in the following field. |
| IP Address | This field is applicable only if you choose the **IP address attached on LAN** method in the **Assigned By** field. Enter the IP address of the computer on the LAN whose MAC you are cloning. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

## 29.3 Dial Backup

The Dial Backup port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. To set up the auxiliary port (Dial Backup) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the Quick Start Guide), then configure

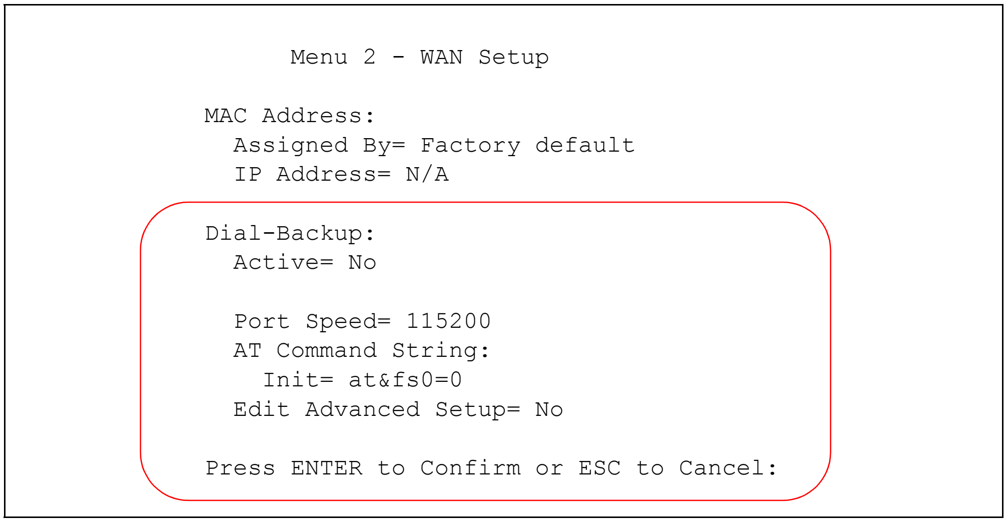
1. Menu 2 - WAN Setup,
2. Menu 2.1 - Advanced WAN Setup and
3. Menu 11.2 - Remote Node Profile (Backup ISP) as shown next

Refer also to the section about traffic redirect for information on an alternate backup WAN connection.

## 29.4 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

**Figure 309** Menu 2: Dial Backup Setup



```
                Menu 2 - WAN Setup

          MAC Address:
            Assigned By= Factory default
            IP Address= N/A

          Dial-Backup:
            Active= No

            Port Speed= 115200
            AT Command String:
              Init= at&fs0=0
            Edit Advanced Setup= No

          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 178** Menu 2: Dial Backup Setup

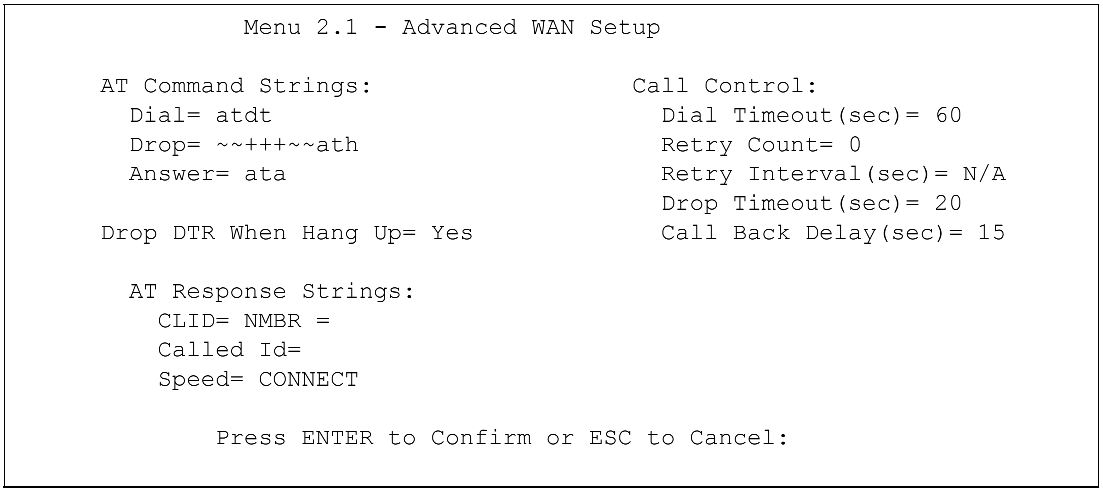
| FIELD | DESCRIPTION |
|---|---|
| Dial-Backup: | |
| Active | Use this field to turn the dial-backup feature on (**Yes**) or off (**No**). |
| Port Speed | Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device.<br>Available speeds are:<br>**9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps. |
| AT Command String: | |
| Init | Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands. |
| Edit Advanced Setup | To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.1 - Advanced Setup**. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

## 29.5 Advanced WAN Setup

Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.

To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2 - WAN Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

**Figure 310** Menu 2.1: Advanced WAN Setup



```
                Menu 2.1 - Advanced WAN Setup

      AT Command Strings:                   Call Control:
        Dial= atdt                            Dial Timeout(sec)= 60
        Drop= ~~+++~~ath                      Retry Count= 0
        Answer= ata                           Retry Interval(sec)= N/A
                                              Drop Timeout(sec)= 20
      Drop DTR When Hang Up= Yes              Call Back Delay(sec)= 15

        AT Response Strings:
          CLID= NMBR =
          Called Id=
          Speed= CONNECT

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes fields in this menu.

**Table 179** Advanced WAN Port Setup: AT Commands Fields

| FIELD | DESCRIPTION |
|---|---|
| AT Command Strings: | |
| Dial | Enter the AT Command string to make a call. |
| Drop | Enter the AT Command string to drop a call. "~" represents a one second wait, e.g., "~~~+++~~ath" can be used if your modem has a slow response time. |
| Answer | Enter the AT Command string to answer a call. |
| Drop DTR When Hang Up | Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the "AT Command String: Drop" is sent out. |
| AT Response Strings: | |
| CLID (Calling Line Identification) | Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication. |
| Called Id | Enter the keyword preceding the dialed number. |
| Speed | Enter the keyword preceding the connection speed. |

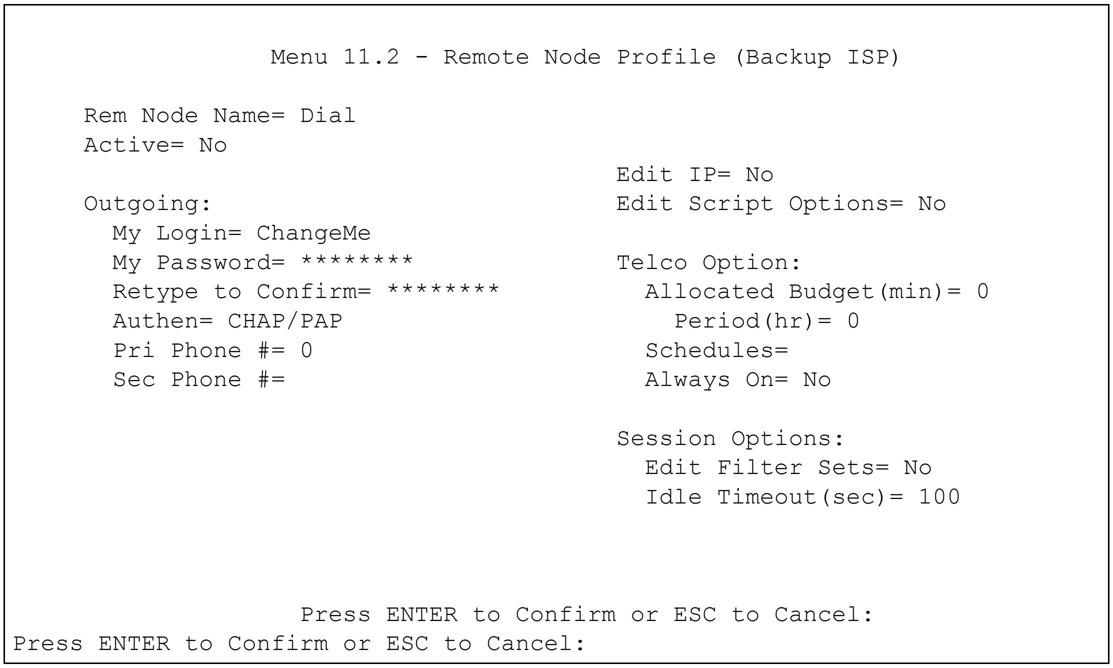
**Table 180** Advanced WAN Port Setup: Call Control Parameters

| FIELD | DESCRIPTION |
|---|---|
| Call Control | |
| Dial Timeout (sec) | Enter a number of seconds for the ZyWALL to keep trying to set up an outgoing call before timing out (stopping). The ZyWALL times out and stops if it cannot set up an outgoing call within the timeout value. |
| Retry Count | Enter a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number. |
| Retry Interval (sec) | Enter a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted. |
| Drop Timeout (sec) | Enter a number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation. |
| Call Back Delay (sec) | Enter a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the co-responding callback call. |

## 29.6 Remote Node Profile (Backup ISP)

On the ZyWALL, enter **2** in **Menu 11 - Remote Node Setup** to open **Menu 11.2 - Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection.

**Figure 311** Menu 11.2: Remote Node Profile (Backup ISP)



```
                  Menu 11.2 - Remote Node Profile (Backup ISP)

     Rem Node Name= Dial
     Active= No
                                          Edit IP= No
     Outgoing:                            Edit Script Options= No
       My Login= ChangeMe
       My Password= ********              Telco Option:
       Retype to Confirm= ********          Allocated Budget(min)= 0
       Authen= CHAP/PAP                       Period(hr)= 0
       Pri Phone #= 0                       Schedules=
       Sec Phone #=                         Always On= No

                                          Session Options:
                                            Edit Filter Sets= No
                                            Idle Timeout(sec)= 100



                    Press ENTER to Confirm or ESC to Cancel:
Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

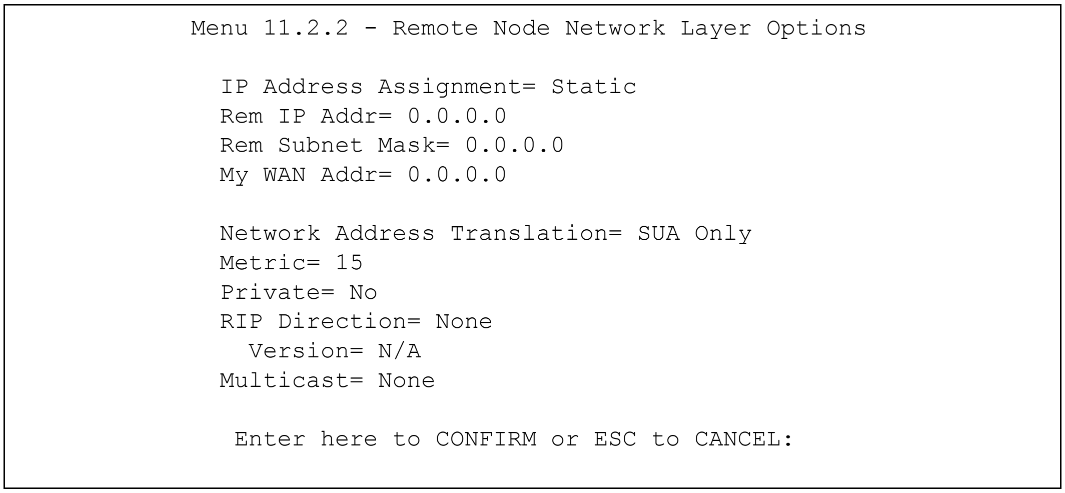
**Table 181** Menu 11.3: Remote Node Profile (Backup ISP)

| FIELD | DESCRIPTION |
|---|---|
| Rem Node Name | Enter a descriptive name for the remote node. This field can be up to eight characters. |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node. |
| Outgoing | |
| My Login | Enter the login name assigned by your ISP for this remote node. |
| My Password | Enter the password assigned by your ISP for this remote node. |
| Retype to Confirm | Enter your password again to make sure that you have entered is correctly. |
| Authen | This field sets the authentication protocol used for outgoing calls.<br>Options for this field are:<br>**CHAP**/**PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node.<br>**CHAP** - accept CHAP only.<br>**PAP** - accept PAP only. |
| Pri Phone #<br>Sec Phone # | Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required. |
| Edit IP | This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.2.2 - Remote Node Network Layer Options**. See Section 29.7 on page 487 for more information. |
| Edit Script Options | Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.2.3 - Remote Node Script**). See Section 29.8 on page 488 for more information. |
| Telco Option | |
| Allocated Budget | Enter the maximum number of minutes that this remote node may be called within the time period configured in the **Period** field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node. |
| Period(hr) | Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour). |
| Schedules | You can apply up to four schedule sets here. For more details please refer to Chapter 44 on page 599. |
| Always On | Press [SPACE BAR] to select **Yes** to set this connection to be on all the time, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection. |
| Session Options | |
| Edit Filter sets | This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.2.4 to edit the filter sets. See Section 29.9 on page 489 for more details. |
| Idle Timeout | Enter the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) that can elapse before the ZyWALL automatically disconnects the PPP connection. This option only applies when the ZyWALL initiates the call. |
| Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel. | |

## 29.7 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.2, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.2.2 - Remote Node Network Layer Options**.

**Figure 312** Menu 11.2.2: Remote Node Network Layer Options



```
                Menu 11.2.2 - Remote Node Network Layer Options

                  IP Address Assignment= Static
                  Rem IP Addr= 0.0.0.0
                  Rem Subnet Mask= 0.0.0.0
                  My WAN Addr= 0.0.0.0

                  Network Address Translation= SUA Only
                  Metric= 15
                  Private= No
                  RIP Direction= None
                    Version= N/A
                  Multicast= None

                   Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

**Table 182** Menu 11.2.2: Remote Node Network Layer Options

| FIELD | DESCRIPTION |
|---|---|
| IP Address Assignment | If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields. |
| Rem IP Address | Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field). |
| Rem Subnet Mask | Enter the subnet mask associated with your static IP. |
| My WAN Addr | Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static).<br>This is the address assigned to your local ZyWALL, not the remote router. |
| Network Address Translation | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Press [SPACE BAR] and then [ENTER] to select either **None** or **SUA Only**.<br>Choose **None** to disable NAT.<br>Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.<br>See Chapter 17 on page 331 for a full discussion on this feature. |
| Metric | Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes. The smaller the number, the higher priority the route has. |

**Table 182** Menu 11.2.2: Remote Node Network Layer Options

| FIELD | DESCRIPTION |
|---|---|
| Private | This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts. |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the **RIP Direction** from **Both**, **None**, **In Only**, **Out Only** and **None**. |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**. |
| Multicast | IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See Section 6.5 on page 135 for more information on this feature. |
| Once you have completed filling in **Menu 11.3.2 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11.3, or press [ESC] at any time to cancel. | |

## 29.8 Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The ZyWALL provides a script facility for this purpose. The script has six programmable sets; each set is composed of an 'Expect' string and a 'Send' string. After matching a message from the server to the 'Expect' field, the ZyWALL returns the set's 'Send' string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
Login: myLogin
Password:
```

To handle the first prompt, you specify "`ogin: `" as the 'Expect' string and "`myLogin`" as the 'Send' string in set 1. The reason for leaving out the leading "`L`" is to avoid having to know exactly whether it is upper or lower case. Similarly, you specify "`word: `" as the 'Expect' string and your password as the 'Send' string for the second prompt in set 2.

You can use two variables, `$USERNAME` and `$PASSWORD` (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear. They are replaced with the outgoing login name and password in the remote node when the ZyWALL sees them in a 'Send' string. Please note that both variables must been entered exactly as shown. No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

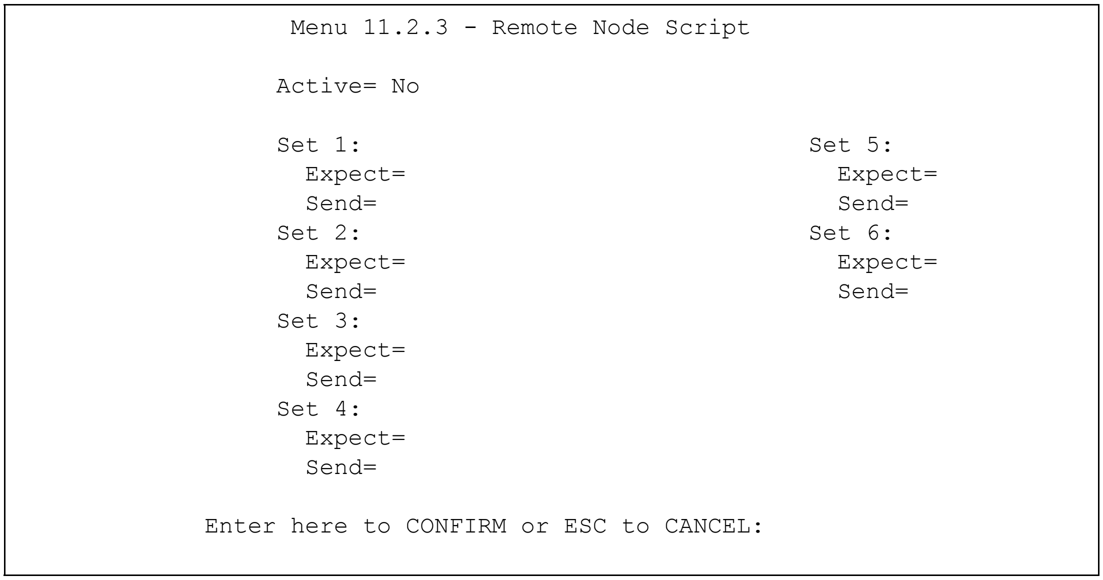
Please note that the ordering of the sets is significant, i.e., starting from set 1, the ZyWALL will wait until the 'Expect' string is matched before it proceeds to set 2, and so on for the rest of the script. When both the 'Expect' and the 'Send' fields of the current set are empty, the ZyWALL will terminate the script processing and start PPP negotiation. This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored. Second, the last set should match the final message sent by the server. For instance, if the server prints:

```
login successful.
Starting PPP...
```

after you enter the password, then you should create a third set to match the final "`PPP...`" but without a "Send" string. Otherwise, the ZyWALL will start PPP prematurely right after sending your password to the server.

If there are errors in the script and it gets stuck at a set for longer than the "Dial Timeout" in menu 2 (default 60 seconds), the ZyWALL will timeout and drop the line. To debug a script, go to Menu 24.4 to initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.

**Figure 313** Menu 11.2.3: Remote Node Script



```
                    Menu 11.2.3 - Remote Node Script

                   Active= No

                   Set 1:                                    Set 5:
                     Expect=                                   Expect=
                     Send=                                     Send=
                   Set 2:                                    Set 6:
                     Expect=                                   Expect=
                     Send=                                     Send=
                   Set 3:
                     Expect=
                     Send=
                   Set 4:
                     Expect=
                     Send=

              Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

**Table 183** Menu 11.2.3: Remote Node Script

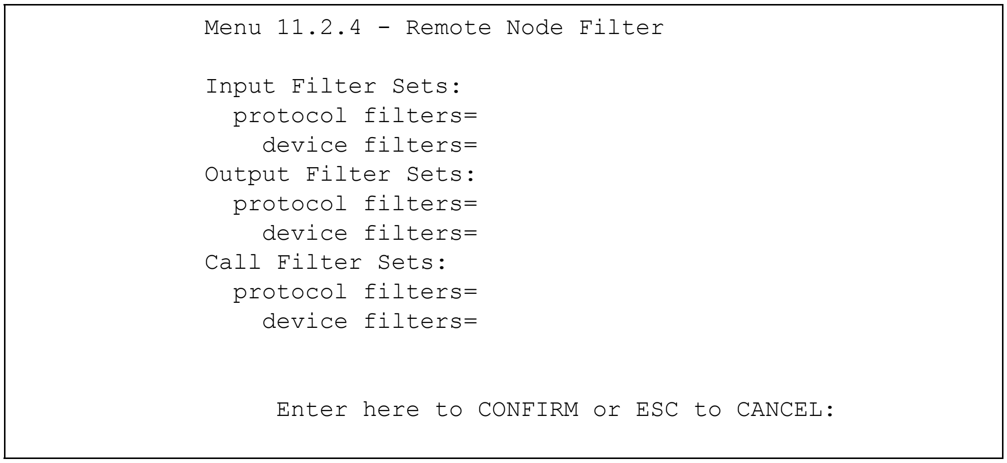
| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] and then [ENTER] to select either **Yes** to enable the AT strings or **No** to disable them. |
| Set 1-6: Expect | Enter an Expect string to match. After matching the Expect string, the ZyWALL returns the string in the **Send** field. |
| Set 1-6: Send | Enter a string to send out after the Expect string is matched. |

## 29.9 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.2, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.2.4 - Remote Node Filter**.

Use menu 11.2.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to Chapter 38 on page 541 for more information on defining the filters.

**Figure 314** Menu 11.2.4: Remote Node Filter



```
              Menu 11.2.4 - Remote Node Filter

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=
              Call Filter Sets:
                protocol filters=
                  device filters=


                   Enter here to CONFIRM or ESC to CANCEL:
```

# 30

# LAN Setup

This chapter describes how to configure the LAN using **Menu 3 - LAN Setup**.

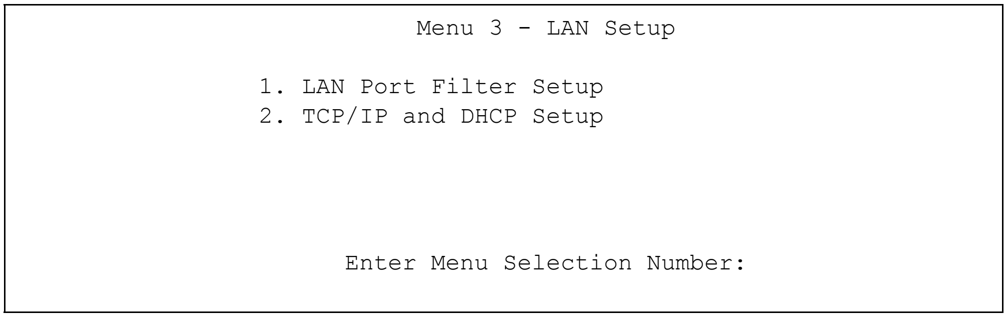
## 30.1 Introduction to LAN Setup

This chapter describes how to configure the ZyWALL for LAN connections.

## 30.2 Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 - LAN Setup**.

**Figure 315** Menu 3: LAN Setup

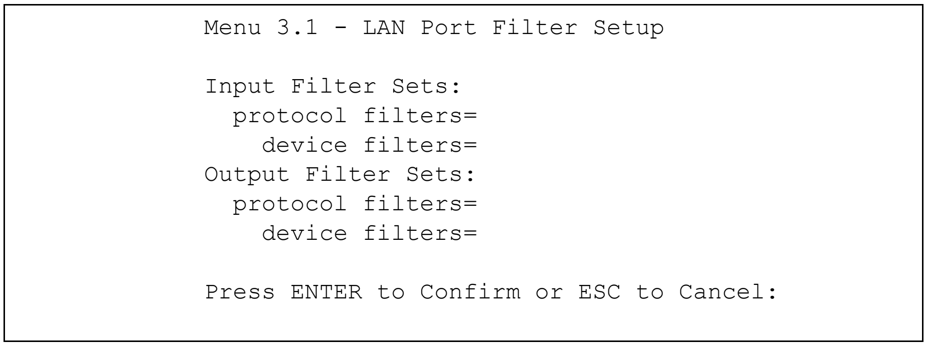


```
                          Menu 3 - LAN Setup

                 1. LAN Port Filter Setup
                 2. TCP/IP and DHCP Setup




                         Enter Menu Selection Number:
```

## 30.3 LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

**Figure 316** Menu 3.1: LAN Port Filter Setup

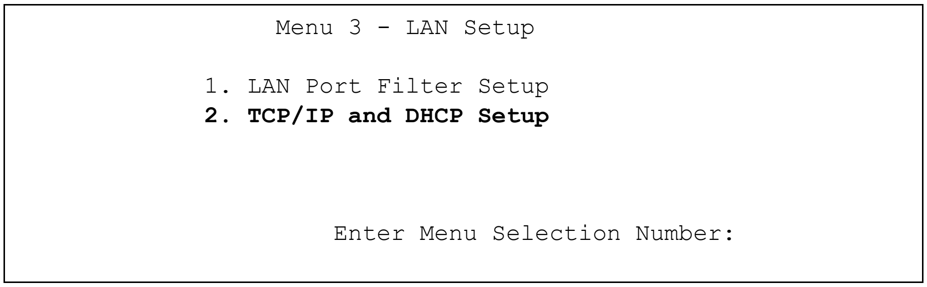


```
              Menu 3.1 - LAN Port Filter Setup

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=

              Press ENTER to Confirm or ESC to Cancel:
```

## 30.4 TCP/IP and DHCP Ethernet Setup Menu

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.

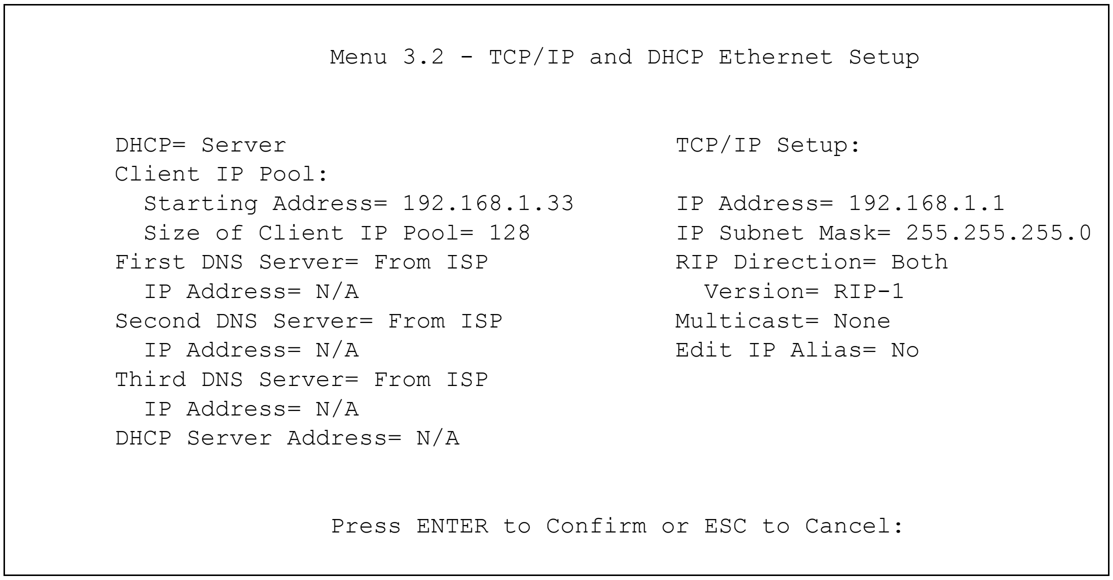
**Figure 317** Menu 3: TCP/IP and DHCP Setup



```
                   Menu 3 - LAN Setup

              1. LAN Port Filter Setup
              2. TCP/IP and DHCP Setup



                       Enter Menu Selection Number:
```

From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**, as shown next. Not all fields are available on all models.

**Figure 318** Menu 3.2: TCP/IP and DHCP Ethernet Setup



```
                      Menu 3.2 - TCP/IP and DHCP Ethernet Setup


       DHCP= Server                           TCP/IP Setup:
       Client IP Pool:
         Starting Address= 192.168.1.33       IP Address= 192.168.1.1
         Size of Client IP Pool= 128          IP Subnet Mask= 255.255.255.0
       First DNS Server= From ISP             RIP Direction= Both
         IP Address= N/A                        Version= RIP-1
       Second DNS Server= From ISP            Multicast= None
         IP Address= N/A                      Edit IP Alias= No
       Third DNS Server= From ISP
         IP Address= N/A
       DHCP Server Address= N/A


                      Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table on how to configure the DHCP fields.

**Table 184** Menu 3.2: DHCP Ethernet Setup Fields

| FIELD | DESCRIPTION |
|---|---|
| DHCP | This field enables or disables the DHCP server.<br>If set to **Server**, your ZyWALL will act as a DHCP server.<br>If set to **None**, the DHCP server will be disabled.<br>If set to **Relay**, the ZyWALL acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients.<br>When set to **Server**, the following items need to be set: |
| Client IP Pool: | |
| Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Size of Client IP Pool | This field specifies the size, or count of the IP address pool. |

**Table 184** Menu 3.2: DHCP Ethernet Setup Fields

| FIELD | DESCRIPTION |
|---|---|
| First DNS Server<br>Second DNS Server<br>Third DNS Server | The ZyWALL passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients.<br>Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyWALL's WAN IP address). The **IP Address** field below displays the (read-only) DNS server IP address that the ISP assigns.<br>Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the **IP Address** field below. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you save your changes. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you save your changes.<br>Select **DNS Relay** to have the ZyWALL act as a DNS proxy. The ZyWALL's LAN IP address displays in the **IP Address** field below (read-only). The ZyWALL tells the DHCP clients on the LAN that the ZyWALL itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyWALL, the ZyWALL forwards the query to the ZyWALL's system DNS server (configured in menu 1) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you save your changes.<br>Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. |
| DHCP Server Address | If **Relay** is selected in the **DHCP** field above, then type the IP address of the actual, remote DHCP server here. |

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

LAN and DMZ IP addresses must be on separate subnets.

**Table 185** Menu 3.2: LAN TCP/IP Setup Fields

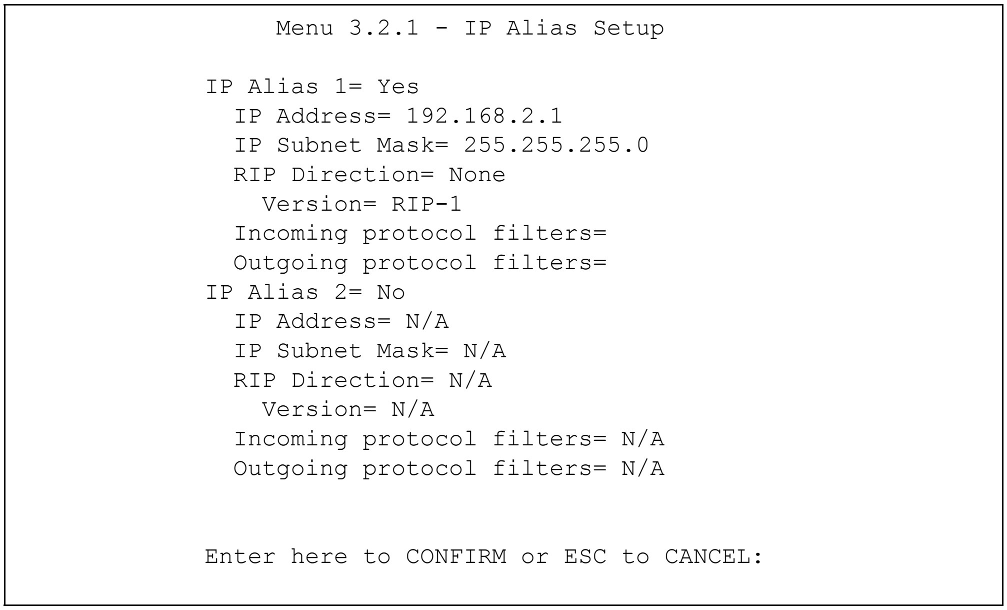
| FIELD | DESCRIPTION |
|---|---|
| TCP/IP Setup: | |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation |
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**. |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**. |
| Multicast | IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select **None** (default) to disable it. |
| Edit IP Alias | The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1 |
| When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel. | |

### 30.4.1 IP Alias Setup

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network.

Use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next. Use this menu to configure the second and third networks.

**Figure 319** Menu 3.2.1: IP Alias Setup



```
     Menu 3.2.1 - IP Alias Setup

IP Alias 1= Yes
  IP Address= 192.168.2.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
    Version= RIP-1
  Incoming protocol filters=
  Outgoing protocol filters=
IP Alias 2= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
    Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A


Enter here to CONFIRM or ESC to CANCEL:
```

Use the instructions in the following table to configure IP alias parameters.

**Table 186** Menu 3.2.1: IP Alias Setup

| FIELD | DESCRIPTION |
|---|---|
| IP Alias 1, 2 | Choose **Yes** to configure the LAN network for the ZyWALL. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation. |
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only**, **Out Only** or **None**. |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**. |
| Incoming Protocol Filters | Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyWALL. |
| Outgoing Protocol Filters | Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyWALL. |
| When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel. | |

# 31

# Internet Access

This chapter shows you how to configure your ZyWALL for Internet access.

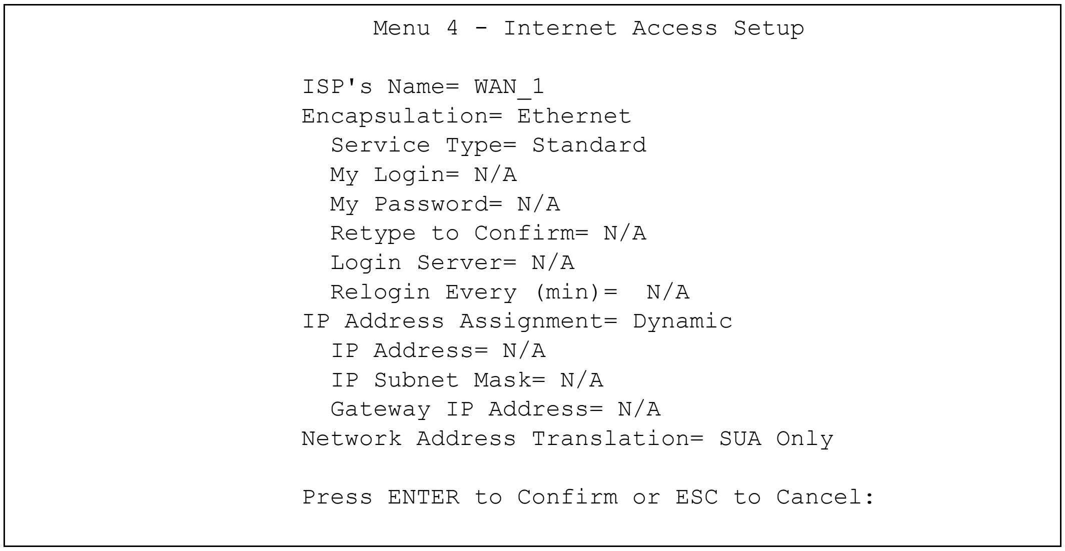
## 31.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your ZyWALL to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet**, **PPTP** or **PPPoE** Encapsulation. Contact your ISP to determine what encapsulation type you should use.

## 31.2 Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next menu.

**Figure 320** Menu 4: Internet Access Setup (Ethernet)



```
                    Menu 4 - Internet Access Setup

               ISP's Name= WAN_1
               Encapsulation= Ethernet
                 Service Type= Standard
                 My Login= N/A
                 My Password= N/A
                 Retype to Confirm= N/A
                 Login Server= N/A
                 Relogin Every (min)=  N/A
               IP Address Assignment= Dynamic
                 IP Address= N/A
                 IP Subnet Mask= N/A
                 Gateway IP Address= N/A
               Network Address Translation= SUA Only

               Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 187** Menu 4: Internet Access Setup (Ethernet)

| FIELD | DESCRIPTION |
|---|---|
| ISP's Name | This is the descriptive name of your ISP for identification purposes. |
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for the **IP Address** field. |
| Service Type | Press [SPACE BAR] and then [ENTER] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**. |
| Note: DSL users must choose the Standard option only. The My Login, My Password and Login Server fields are not applicable in this case. | |
| My Login | Enter the login name given to you by your ISP. |
| My Password | Type your password again for confirmation. |
| Retype to Confirm | Enter your password again to make sure that you have entered is correctly. |
| Login Server | The ZyWALL will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address. |
| Relogin Every (min) | This field is available when you select **Telia Login** in the **Service Type** field.<br>The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyWALL to wait between logins. |
| IP Address Assignment | If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields. |
| IP Address | Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field). |
| IP Subnet Mask | Enter the subnet mask associated with your static IP. |
| Gateway IP Address | Enter the gateway IP address associated with your static IP. |
| Network Address Translation | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Choose **None** to disable NAT.<br>Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.<br>Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set!<br>Please see Chapter 17 on page 331 for a more detailed discussion on the Network Address Translation feature. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

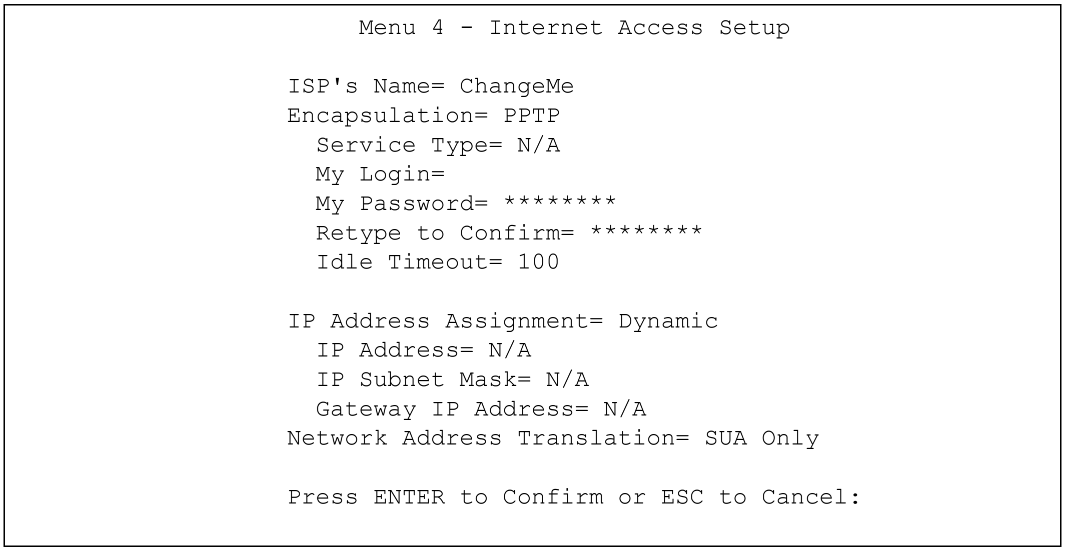
## 31.3 Configuring the PPTP Client

The ZyWALL supports only one PPTP server connection at any given time.

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

**Figure 321** Internet Access Setup (PPTP)



```
     Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPTP
  Service Type= N/A
  My Login=
  My Password= ********
  Retype to Confirm= ********
  Idle Timeout= 100

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

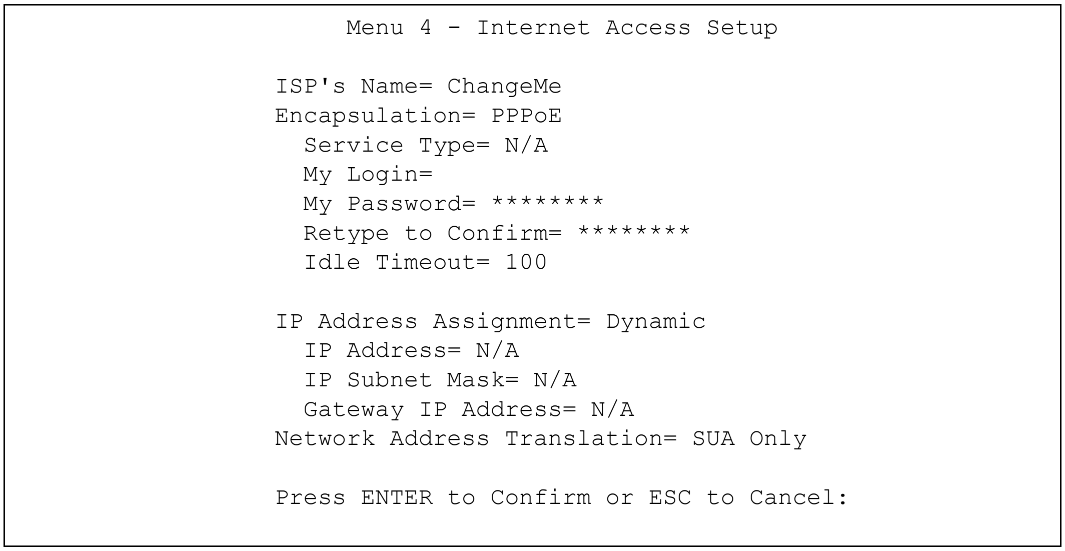
**Table 188** New Fields in Menu 4 (PPTP) Screen

| FIELD | DESCRIPTION |
|---|---|
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose **PPTP**. The encapsulation method influences your choices for the **IP Address** field. |
| Idle Timeout | This value specifies the time, in seconds, that elapses before the ZyWALL automatically disconnects from the PPTP server. |

## 31.4 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen.

**Figure 322** Internet Access Setup (PPPoE)



```
                         Menu 4 - Internet Access Setup

                    ISP's Name= ChangeMe
                    Encapsulation= PPPoE
                      Service Type= N/A
                      My Login=
                      My Password= ********
                      Retype to Confirm= ********
                      Idle Timeout= 100

                    IP Address Assignment= Dynamic
                      IP Address= N/A
                      IP Subnet Mask= N/A
                      Gateway IP Address= N/A
                    Network Address Translation= SUA Only

                    Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions about the new fields when you choose **PPPoE** in the **Encapsulation** field in menu 4.

**Table 189** New Fields in Menu 4 (PPPoE) screen

| FIELD | DESCRIPTION |
|---|---|
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices in the **IP Address** field. |
| Idle Timeout | This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server. |

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

## 31.5 Basic Setup Complete

Well done! You have successfully connected, installed and set up your ZyWALL to operate on your network as well as access the Internet.

When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

You may deactivate the firewall in menu 21.2 or via the ZyWALL embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the chapters on firewall for more information on the firewall.

# 32

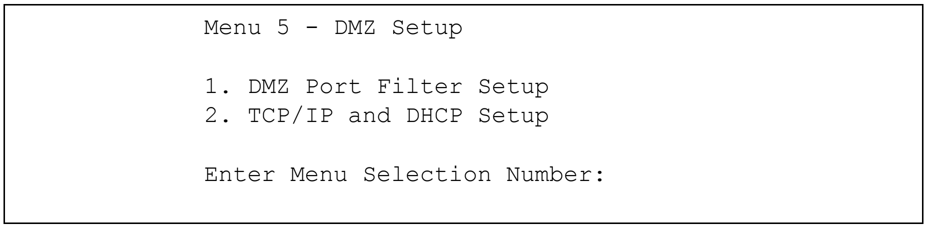
# DMZ Setup

This chapter describes how to configure the ZyWALL’s DMZ using **Menu 5 - DMZ Setup**.

## 32.1 Configuring DMZ Setup

From the main menu, enter 5 to open **Menu 5 – DMZ Setup**.

**Figure 323** Menu 5: DMZ Setup

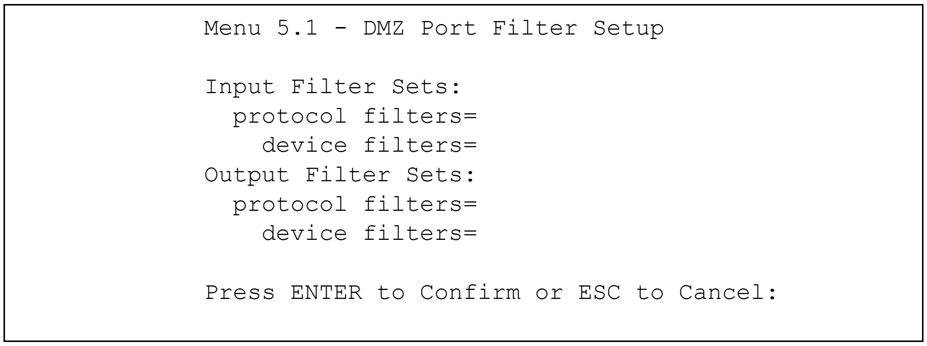


```
Menu 5 - DMZ Setup

1. DMZ Port Filter Setup
2. TCP/IP and DHCP Setup

Enter Menu Selection Number:
```

## 32.2 DMZ Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to your public server(s) traffic.

**Figure 324** Menu 5.1: DMZ Port Filter Setup



```
Menu 5.1 - DMZ Port Filter Setup

Input Filter Sets:
  protocol filters=
    device filters=
Output Filter Sets:
  protocol filters=
    device filters=

Press ENTER to Confirm or ESC to Cancel:
```

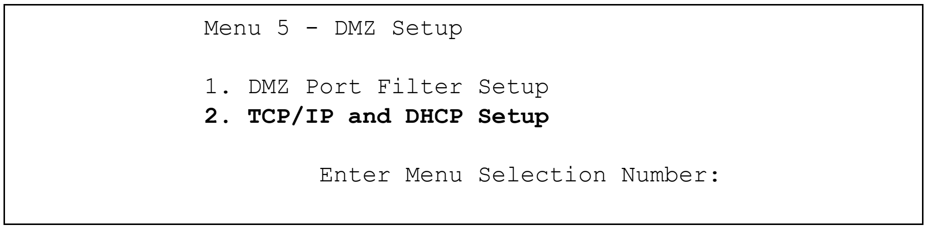
## 32.3 TCP/IP Setup

For more detailed information about RIP setup, IP multicast and IP alias, please refer to Chapter 6 on page 133.

### 32.3.1 IP Address

From the main menu, enter 5 to open **Menu 5 - DMZ Setup** to configure TCP/IP (RFC 1155).

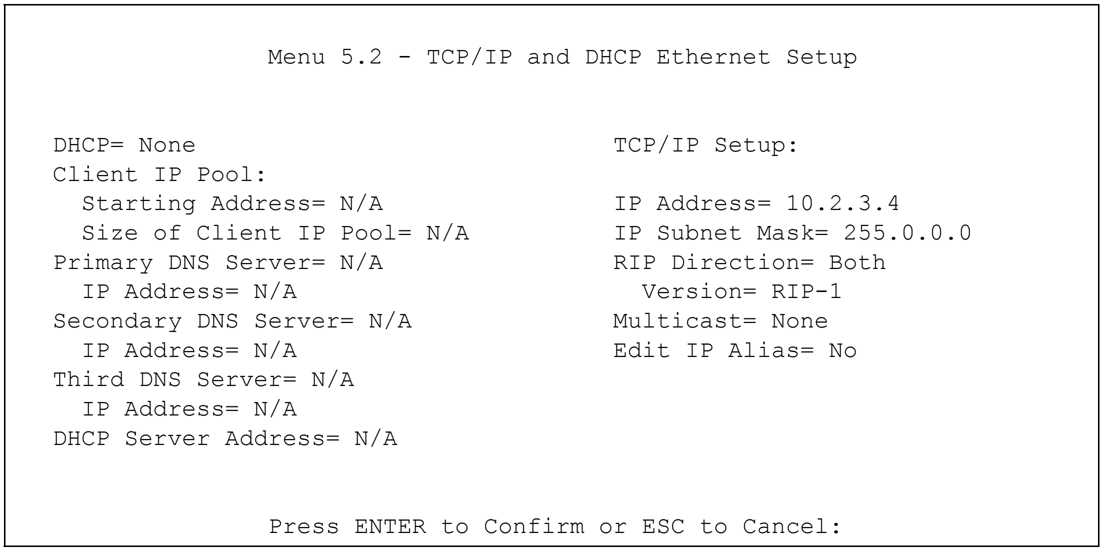
**Figure 325** Menu 5: DMZ Setup



```
              Menu 5 - DMZ Setup

              1. DMZ Port Filter Setup
              2. TCP/IP and DHCP Setup

                      Enter Menu Selection Number:
```

From menu 5, select the submenu option **2. TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 5.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

**Figure 326** Menu 5.2: TCP/IP and DHCP Ethernet Setup



```
                 Menu 5.2 - TCP/IP and DHCP Ethernet Setup


   DHCP= None                                 TCP/IP Setup:
   Client IP Pool:
     Starting Address= N/A                    IP Address= 10.2.3.4
     Size of Client IP Pool= N/A              IP Subnet Mask= 255.0.0.0
   Primary DNS Server= N/A                    RIP Direction= Both
     IP Address= N/A                            Version= RIP-1
   Secondary DNS Server= N/A                  Multicast= None
     IP Address= N/A                          Edit IP Alias= No
   Third DNS Server= N/A
     IP Address= N/A
   DHCP Server Address= N/A


                 Press ENTER to Confirm or ESC to Cancel:
```

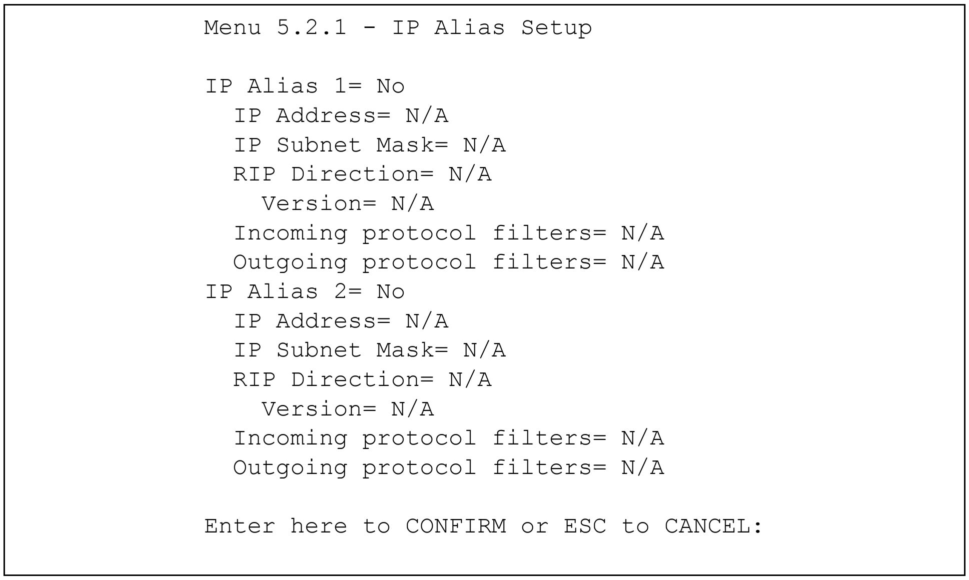
The DHCP and TCP/IP setup fields are the same as the ones in **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**. Each public server will need a unique IP address. Refer to Section 30.4 on page 492 for information on how to configure these fields.

DMZ, WLAN and LAN IP addresses must be on separate subnets. You must also configure NAT for the DMZ port (see Chapter 36 on page 521) in menus 15.1 and 15.2.

## 32.3.2 IP Alias Setup

Use menu 5.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to open **Menu 5.2.1 - IP Alias Setup**, as shown next. Use this menu to configure the second and third networks.

**Figure 327** Menu 5.2.1: IP Alias Setup



```
Menu 5.2.1 - IP Alias Setup

IP Alias 1= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
    Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A
IP Alias 2= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
    Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A

Enter here to CONFIRM or ESC to CANCEL:
```

Refer to Table 186 on page 495 for instructions on configuring IP alias parameters.

# 33

# Wireless Setup

Use menu 7 to configure the IP address for ZyWALL's WLAN interface, other TCP/IP and DHCP settings.

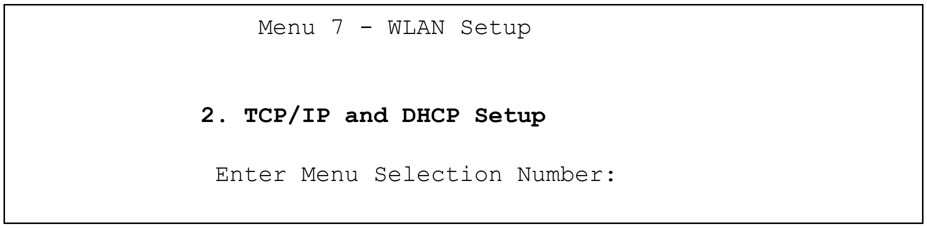
## 33.1 TCP/IP Setup

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to Chapter 6 on page 133.

### 33.1.1 IP Address

From the main menu, enter 7 to open **Menu 7 - WLAN Setup** to configure TCP/IP (RFC 1155).

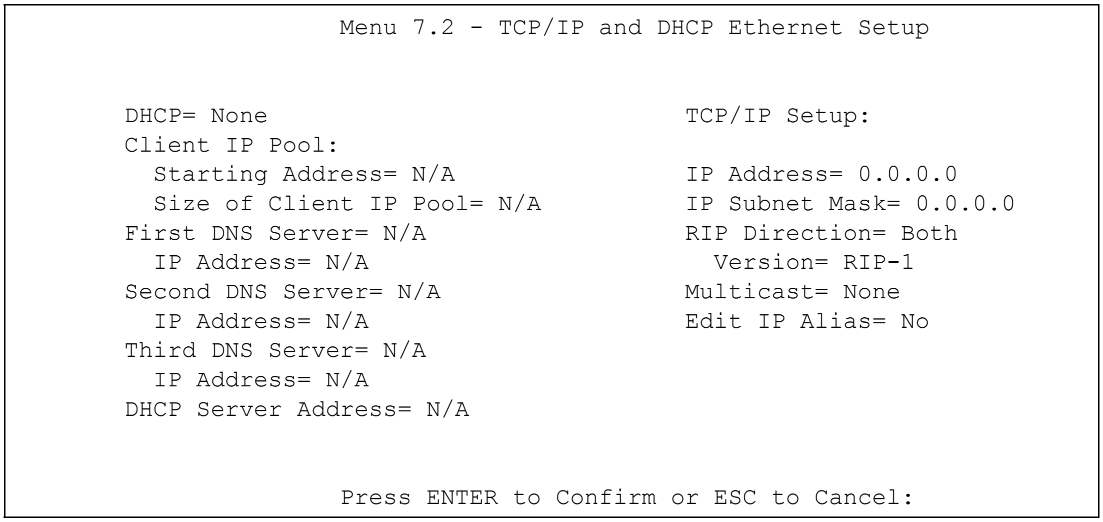
**Figure 328** Menu 7: WLAN Setup



```
                  Menu 7 - WLAN Setup


              2. TCP/IP and DHCP Setup

               Enter Menu Selection Number:
```

From menu 7, select the submenu option **2. TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 7.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

**Figure 329** Menu 7.2: TCP/IP and DHCP Ethernet Setup



```
                       Menu 7.2 - TCP/IP and DHCP Ethernet Setup


        DHCP= None                             TCP/IP Setup:
        Client IP Pool:
          Starting Address= N/A                IP Address= 0.0.0.0
          Size of Client IP Pool= N/A          IP Subnet Mask= 0.0.0.0
        First DNS Server= N/A                  RIP Direction= Both
          IP Address= N/A                        Version= RIP-1
        Second DNS Server= N/A                 Multicast= None
          IP Address= N/A                      Edit IP Alias= No
        Third DNS Server= N/A
          IP Address= N/A
        DHCP Server Address= N/A


                       Press ENTER to Confirm or ESC to Cancel:
```

The DHCP and TCP/IP setup fields are the same as the ones in **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**. Each public server will need a unique IP address. Refer to Section 30.4 on page 492 for information on how to configure these fields.

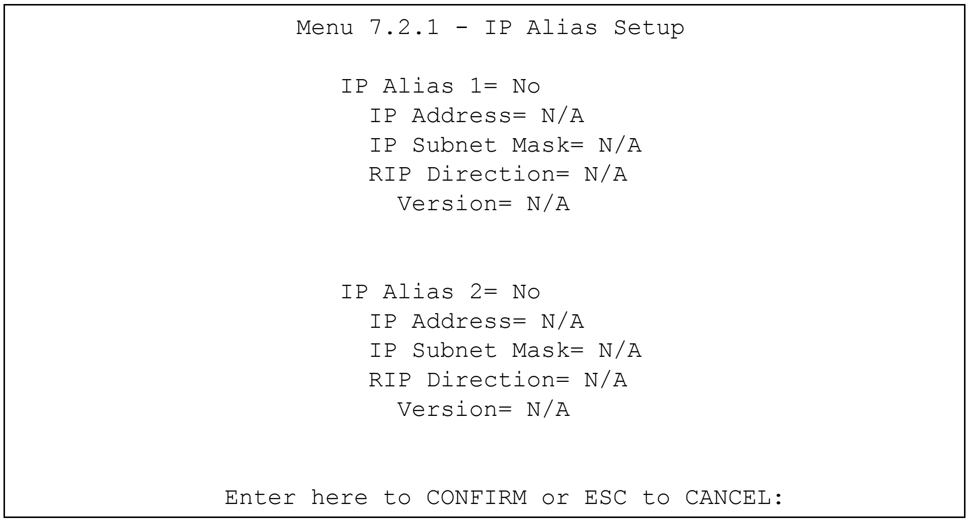
DMZ, WLAN and LAN IP addresses must be on separate subnets. You must also configure NAT for the WLAN port (see Chapter 36 on page 521) in menus 15.1 and 15.2.

## 33.1.2 IP Alias Setup

You must use menu 7.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Pressing [ENTER] opens **Menu 7.2.1 - IP Alias Setup**, as shown next.

**Figure 330** Menu 7.2.1: IP Alias Setup



```
                    Menu 7.2.1 - IP Alias Setup

                       IP Alias 1= No
                         IP Address= N/A
                         IP Subnet Mask= N/A
                         RIP Direction= N/A
                           Version= N/A


                       IP Alias 2= No
                         IP Address= N/A
                         IP Subnet Mask= N/A
                         RIP Direction= N/A
                           Version= N/A


               Enter here to CONFIRM or ESC to CANCEL:
```

Refer to Table 186 on page 495 for instructions on configuring IP alias parameters.

# 34

# Remote Node Setup

This chapter shows you how to configure a remote node.

## 34.1 Introduction to Remote Node Setup

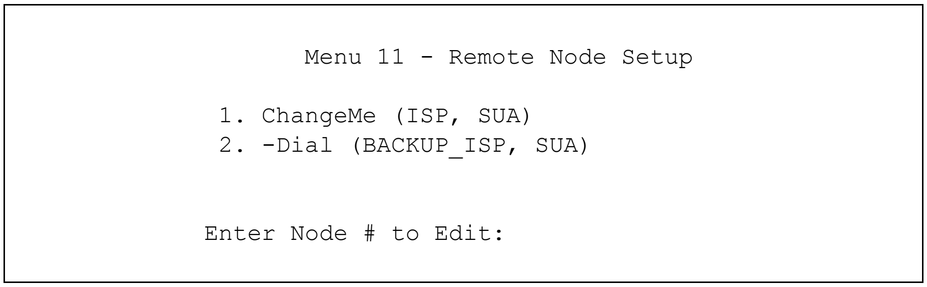
A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 - Remote Node Profile**, **Menu 11.1.2 - Remote Node Network Layer Options** and **Menu 11.1.4 - Remote Node Filter**.

## 34.2 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 - Remote Node Setup** (shown below).

Enter **1** to open **Menu 11.1 - Remote Node Profile** and configure the setup for your WAN port. Enter **2** to open **Menu 11.2 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection (see Chapter 29 on page 481).

**Figure 331** Menu 11: Remote Node Setup



```
                    Menu 11 - Remote Node Setup

                 1. ChangeMe (ISP, SUA)
                 2. -Dial (BACKUP_ISP, SUA)


                Enter Node # to Edit:
```

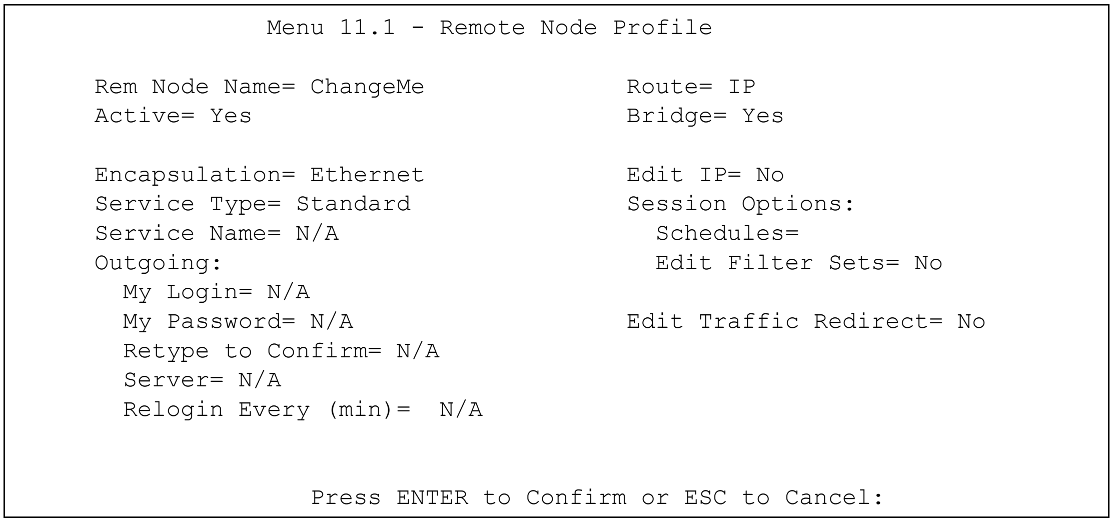
## 34.3 Remote Node Profile Setup

The following explains how to configure the remote node profile menu.

## 34.3.1 Ethernet Encapsulation

There are three variations of menu 11.1 depending on whether you choose **Ethernet Encapsulation**, **PPPoE Encapsulation** or **PPTP Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

**Figure 332** Menu 11.1: Remote Node Profile for Ethernet Encapsulation



```
                Menu 11.1 - Remote Node Profile

    Rem Node Name= ChangeMe             Route= IP
    Active= Yes                         Bridge= Yes

    Encapsulation= Ethernet             Edit IP= No
    Service Type= Standard              Session Options:
    Service Name= N/A                     Schedules=
    Outgoing:                             Edit Filter Sets= No
      My Login= N/A
      My Password= N/A                  Edit Traffic Redirect= No
      Retype to Confirm= N/A
      Server= N/A
      Relogin Every (min)=  N/A


                   Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 190** Menu 11.1: Remote Node Profile for Ethernet Encapsulation

| FIELD | DESCRIPTION |
|---|---|
| Rem Node Name | Enter a descriptive name for the remote node. This field can be up to eight characters. |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node). |
| Encapsulation | **Ethernet** is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to **PPPoE** or **PPTP** encapsulation. |
| Service Type | Press [SPACE BAR] and then [ENTER] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**. |
| Outgoing | |
| My Login | This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the ZyWALL calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server. |
| My Password | Enter the password assigned by your ISP when the ZyWALL calls this remote node. Valid for **PPPoE** encapsulation only. |
| Retype to Confirm | Type your password again to make sure that you have entered it correctly. |

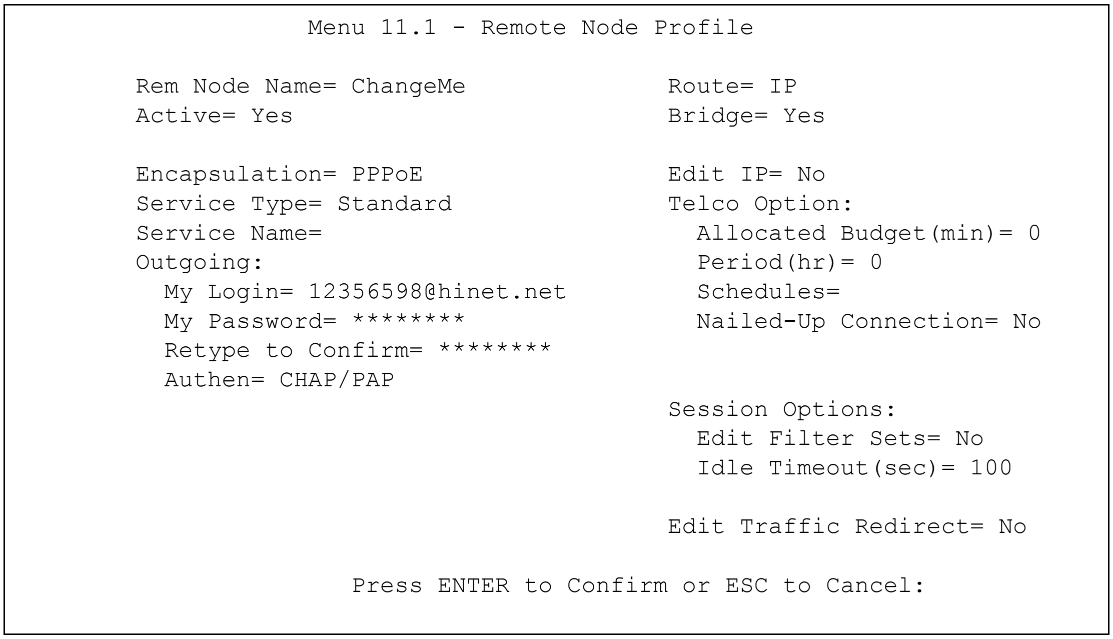
**Table 190** Menu 11.1: Remote Node Profile for Ethernet Encapsulation (continued)

| FIELD | DESCRIPTION |
|---|---|
| Server | This field is valid only when **RoadRunner** is selected in the **Service Type** field. The ZyWALL will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here. |
| Relogin Every (min) | This field is available when you select **Telia Login** in the **Service Type** field.<br>The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyWALL to wait between logins. |
| Route | This field refers to the protocol that will be routed by your ZyWALL – IP is the only option for the ZyWALL. |
| Edit IP | This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.1.2 - Remote Node Network Layer Options**. |
| Session Options | |
| Schedules | You can apply up to four schedule sets here. For more details please refer to Chapter 44 on page 599. |
| Edit Filter Sets | This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.x.4 to edit the filter sets. See Section 34.5 on page 516 for more details. |
| Edit Traffic Redirect | Press [SPACE BAR] to select **Yes** or **No**.<br>Select **No** (default) if you do not want to configure this feature. Select Yes and press [ENTER] to configure **Menu 11.1.5 - Traffic Redirect Setup**. |
| Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel. | |

## 34.3.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you’re using the ZyWALL with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE,** then you will see the next screen.

**Figure 333** Menu 11.1: Remote Node Profile for PPPoE Encapsulation



```
                    Menu 11.1 - Remote Node Profile

        Rem Node Name= ChangeMe             Route= IP
        Active= Yes                         Bridge= Yes

        Encapsulation= PPPoE                Edit IP= No
        Service Type= Standard              Telco Option:
        Service Name=                         Allocated Budget(min)= 0
        Outgoing:                             Period(hr)= 0
          My Login= 12356598@hinet.net        Schedules=
          My Password= ********               Nailed-Up Connection= No
          Retype to Confirm= ********
          Authen= CHAP/PAP
                                            Session Options:
                                              Edit Filter Sets= No
                                              Idle Timeout(sec)= 100

                                            Edit Traffic Redirect= No

                       Press ENTER to Confirm or ESC to Cancel:
```

### 34.3.2.1 Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

### 34.3.2.2 Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyWALL does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyWALL will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields not already described in Table 190 on page 510.

#### 34.3.2.3 Metric

See Section 8.2 on page 151 for details on the **Metric** field.

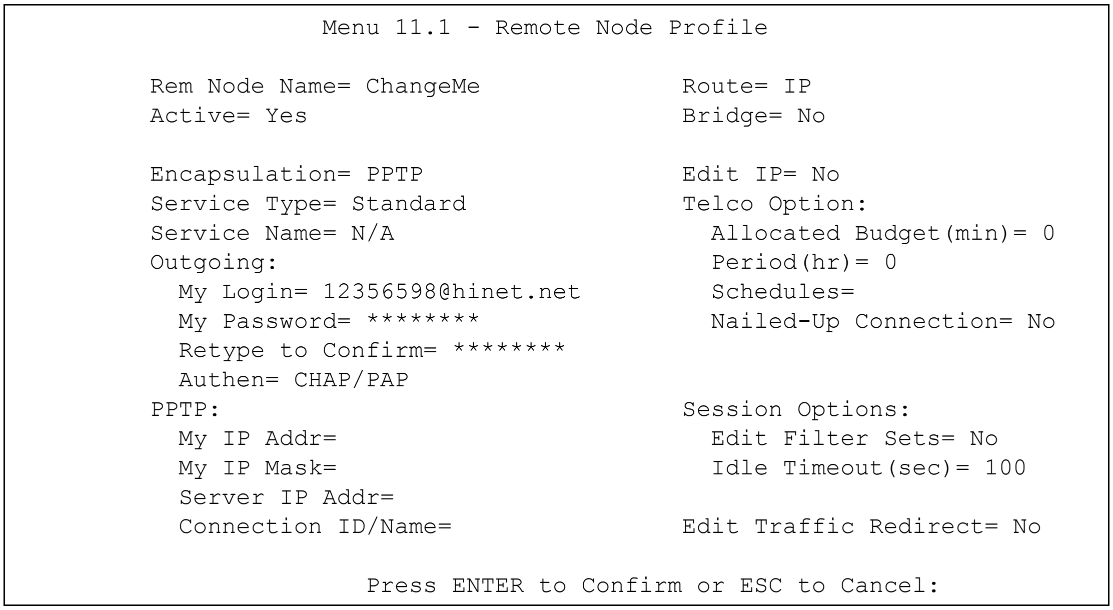
**Table 191** Fields in Menu 11.1 (PPPoE Encapsulation Specific)

| FIELD | DESCRIPTION |
|---|---|
| Service Name | If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation. |
| Authen | This field sets the authentication protocol used for outgoing calls.<br>Options for this field are:<br>**CHAP**/**PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node.<br>**CHAP** - accept CHAP only.<br>**PAP** - accept PAP only. |
| Telco Option | |
| Allocated Budget | The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control. |
| Period(hr) | This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period(hr)** is 1 (hour). |
| Schedules | You can apply up to four schedule sets here. For more details please refer to Chapter 44 on page 599. |
| Nailed-Up Connection | This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section. |
| Session Options | |
| Idle Timeout | Type the length of idle time (when there is no traffic from the ZyWALL to the remote node) in seconds that can elapse before the ZyWALL automatically disconnects the PPPoE connection. This option only applies when the ZyWALL initiates the call. |

### 34.3.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen.

**Figure 334** Menu 11.1: Remote Node Profile for PPTP Encapsulation



```
                      Menu 11.1 - Remote Node Profile

          Rem Node Name= ChangeMe                   Route= IP
          Active= Yes                               Bridge= No

          Encapsulation= PPTP                       Edit IP= No
          Service Type= Standard                    Telco Option:
          Service Name= N/A                           Allocated Budget(min)= 0
          Outgoing:                                   Period(hr)= 0
            My Login= 12356598@hinet.net              Schedules=
            My Password= ********                     Nailed-Up Connection= No
            Retype to Confirm= ********
            Authen= CHAP/PAP
          PPTP:                                     Session Options:
            My IP Addr=                               Edit Filter Sets= No
            My IP Mask=                               Idle Timeout(sec)= 100
            Server IP Addr=
            Connection ID/Name=                     Edit Traffic Redirect= No

                         Press ENTER to Confirm or ESC to Cancel:
```

The next table shows how to configure fields in menu 11.1 not previously discussed.

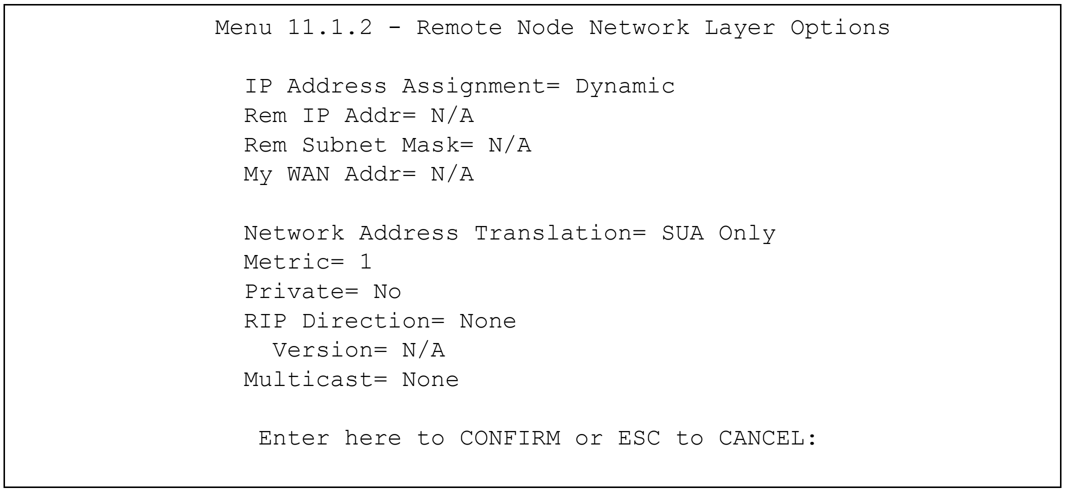
**Table 192** Menu 11.1: Remote Node Profile for PPTP Encapsulation

| FIELD | DESCRIPTION |
|---|---|
| Encapsulation | Press [SPACE BAR] and then [ENTER] to select **PPTP**. You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method. |
| My IP Addr | Enter the IP address of the WAN Ethernet port. |
| My IP Mask | Enter the subnet mask of the WAN Ethernet port. |
| Server IP Addr | Enter the IP address of the ANT modem. |
| Connection ID/ Name | Enter the connection ID or connection name in the ANT. It must follow the “c:id” and “n:name” format.<br>This field is optional and depends on the requirements of your DSL modem. |
| Schedules | You can apply up to four schedule sets here. For more details refer to Chapter 44 on page 599. |
| Nailed-Up Connections | Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to make the connection to this remote node a nailed-up connection. |

## 34.4 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.1.2 - Remote Node Network Layer Options**. Not all fields are available on all models.

**Figure 335** Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation



```
                Menu 11.1.2 - Remote Node Network Layer Options

                  IP Address Assignment= Dynamic
                  Rem IP Addr= N/A
                  Rem Subnet Mask= N/A
                  My WAN Addr= N/A

                  Network Address Translation= SUA Only
                  Metric= 1
                  Private= No
                  RIP Direction= None
                    Version= N/A
                  Multicast= None

                   Enter here to CONFIRM or ESC to CANCEL:
```

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this menu.

**Table 193** Remote Node Network Layer Options Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| IP Address Assignment | If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields. |
| (Rem) IP Address | If you have a static IP Assignment, enter the IP address assigned to you by your ISP. |
| (Rem) IP Subnet Mask | If you have a static IP Assignment, enter the subnet mask assigned to you. |
| Gateway IP Addr | This field is applicable to **Ethernet** encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address. |
| My WAN Addr | This field is applicable to **PPPoE** and **PPTP** encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your ZyWALL.<br>Note that this is the address assigned to your local ZyWALL, not the remote router. |
| Network Address Translation | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Choose **None** to disable NAT.<br>Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.<br>Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set.<br>See Chapter 17 on page 331 for a full discussion on this feature. |

**Table 193** Remote Node Network Layer Options Menu Fields (continued)

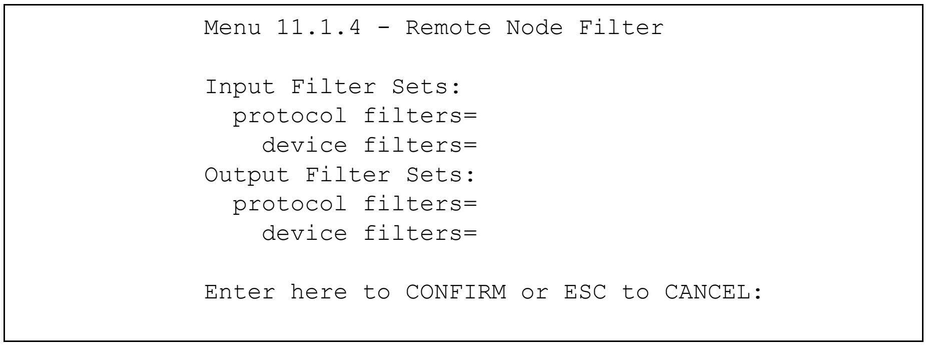
| FIELD | DESCRIPTION |
|---|---|
| Metric | Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see Section 8.2 on page 151). The smaller the number, the higher priority the route has. |
| Private | This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts. |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. See Chapter 6 on page 133 for more information on RIP. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting. |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/ **RIP-2M** or **None**. |
| Multicast | IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2)**. Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See Chapter 6 on page 133 for more information on this feature. |
| Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel. | |

## 34.5 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.1.4 - Remote Node Filter**.

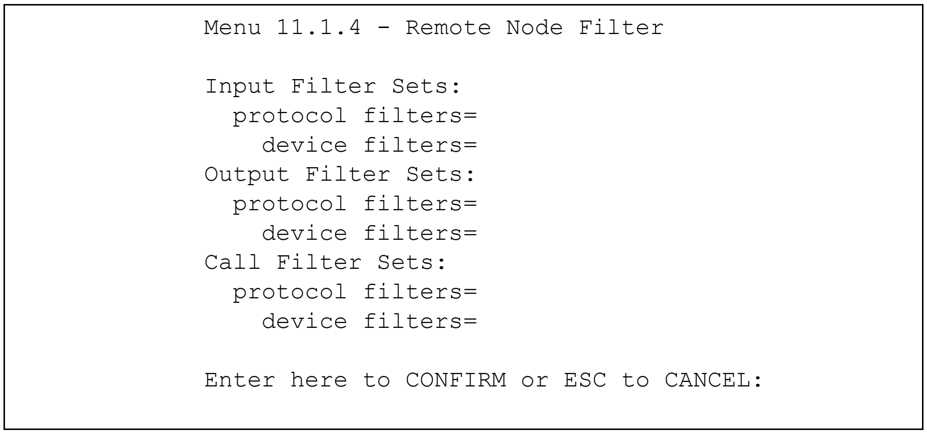
Use menu 11.1.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to Chapter 38 on page 541. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 336** Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation)



```
             Menu 11.1.4 - Remote Node Filter

             Input Filter Sets:
               protocol filters=
                 device filters=
             Output Filter Sets:
               protocol filters=
                 device filters=

             Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 337** Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation)

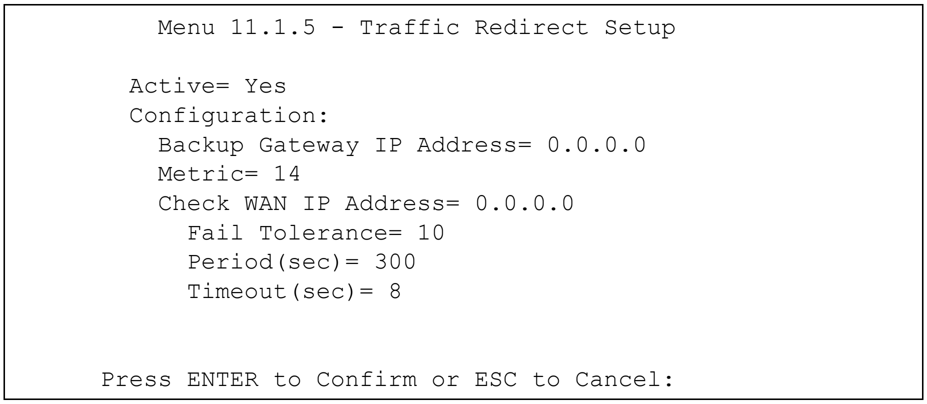


```
Menu 11.1.4 - Remote Node Filter

Input Filter Sets:
  protocol filters=
    device filters=
Output Filter Sets:
  protocol filters=
    device filters=
Call Filter Sets:
  protocol filters=
    device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

## 34.6 Traffic Redirect

Configure parameters that determine when the ZyWALL will forward WAN traffic to the backup gateway using **Menu 11.1.5 - Traffic Redirect Setup**.

**Figure 338** Menu 11.1.5: Traffic Redirect Setup



```
      Menu 11.1.5 - Traffic Redirect Setup

    Active= Yes
    Configuration:
      Backup Gateway IP Address= 0.0.0.0
      Metric= 14
      Check WAN IP Address= 0.0.0.0
        Fail Tolerance= 10
        Period(sec)= 300
        Timeout(sec)= 8


  Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 194** Menu 11.1.5: Traffic Redirect Setup

| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] and select Yes (to enable) or No (to disable) traffic redirect setup. The default is No. |
| Configuration | |
| Backup Gateway IP Address | Enter the IP address of your backup gateway in dotted decimal notation.<br>The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates. |
| Metric | This field sets this route's priority among the routes the ZyWALL uses.<br>Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see Section 8.2 on page 151) The smaller the number, the higher priority the route has. |

**Table 194** Menu 11.1.5: Traffic Redirect Setup

| FIELD | DESCRIPTION |
|---|---|
| Check WAN IP Address | Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your ZyWALL's WAN accessibility.<br>The ZyWALL uses the default gateway IP address if you do not enter an IP address here.<br>If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the ZyWALL to check the PVC (Permanent Virtual Circuit) or PPTP tunnel. |
| Fail Tolerance | Enter the number of times your ZyWALL may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number. |
| Period(sec) | Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number. |
| Timeout(sec) | Enter the number of seconds the ZyWALL waits for a ping response from the IP Address in the **Check WAN IP Address** field before it times out. The number in this field should be less than the number in the **Period** field. Three to 50 is usually a good number.<br>The WAN connection is considered "down" after the ZyWALL times out the number of times specified in the **Fail Tolerance** field. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

# 35

# IP Static Route Setup

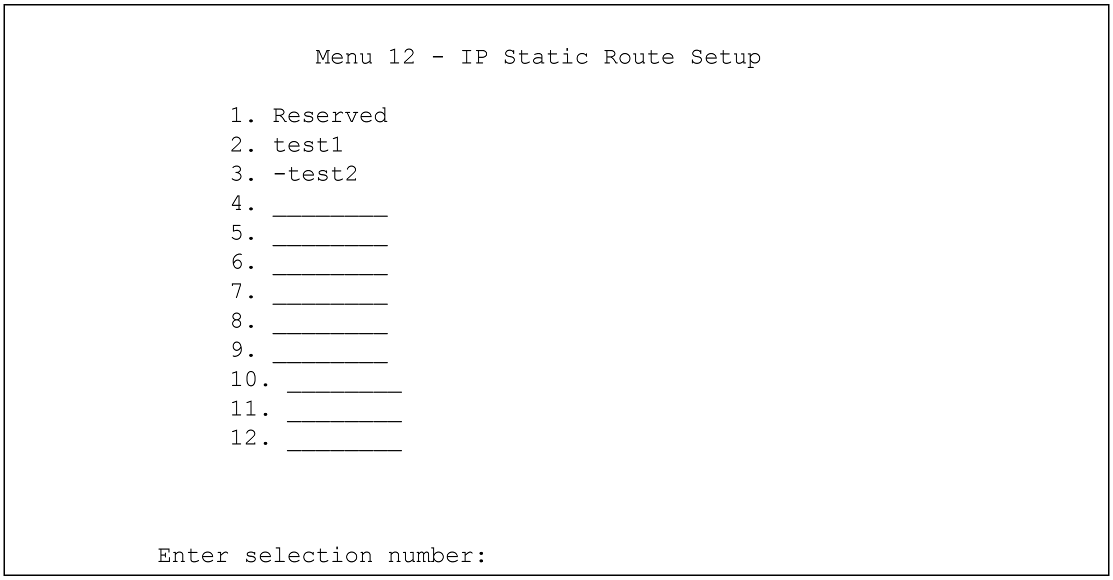
This chapter shows you how to configure static routes with your ZyWALL.

## 35.1 IP Static Route Setup

Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12.1.

The first static route entry is for the default WAN route on the ZyWALL. You cannot modify or delete a static default route. The default route is disabled after you change the static WAN IP address to a dynamic WAN IP address. The “-” before a route name indicates the static route is inactive.

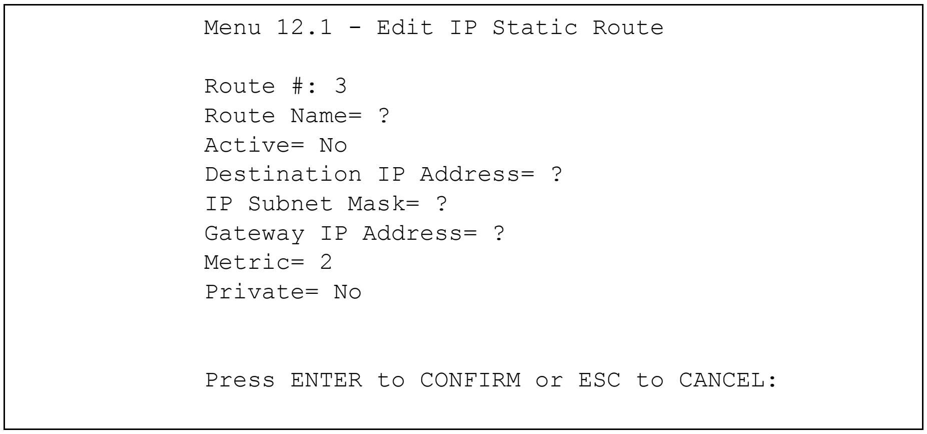
**Figure 339** Menu 12: IP Static Route Setup



```
                    Menu 12 - IP Static Route Setup

              1. Reserved
              2. test1
              3. -test2
              4. ________
              5. ________
              6. ________
              7. ________
              8. ________
              9. ________
              10. ________
              11. ________
              12. ________



          Enter selection number:
```

Now, enter the index number of the static route that you want to configure.

**Figure 340** Menu 12. 1: Edit IP Static Route



```
              Menu 12.1 - Edit IP Static Route

              Route #: 3
              Route Name= ?
              Active= No
              Destination IP Address= ?
              IP Subnet Mask= ?
              Gateway IP Address= ?
              Metric= 2
              Private= No


              Press ENTER to CONFIRM or ESC to CANCEL:
```

`The following table describes the IP Static Route Menu fields.

**Table 195** Menu 12. 1: Edit IP Static Route

| FIELD | DESCRIPTION |
|---|---|
| Route # | This is the index number of the static route that you chose in menu 12. |
| Route Name | Enter a descriptive name for this route. This is for identification purposes only. |
| Active | This field allows you to activate/deactivate this static route. |
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| IP Subnet Mask | Enter the IP subnet mask for this destination. |
| Gateway IP Address | Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the remote nodes. |
| Metric | Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see Section 8.2 on page 151). The smaller the number, the higher priority the route has. |
| Private | This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts. |
| Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel. | |

# 36

# Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

## 36.1 Using NAT

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyWALL.

### 36.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See Section 36.2.1 on page 523 for a detailed description of the NAT set for SUA. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

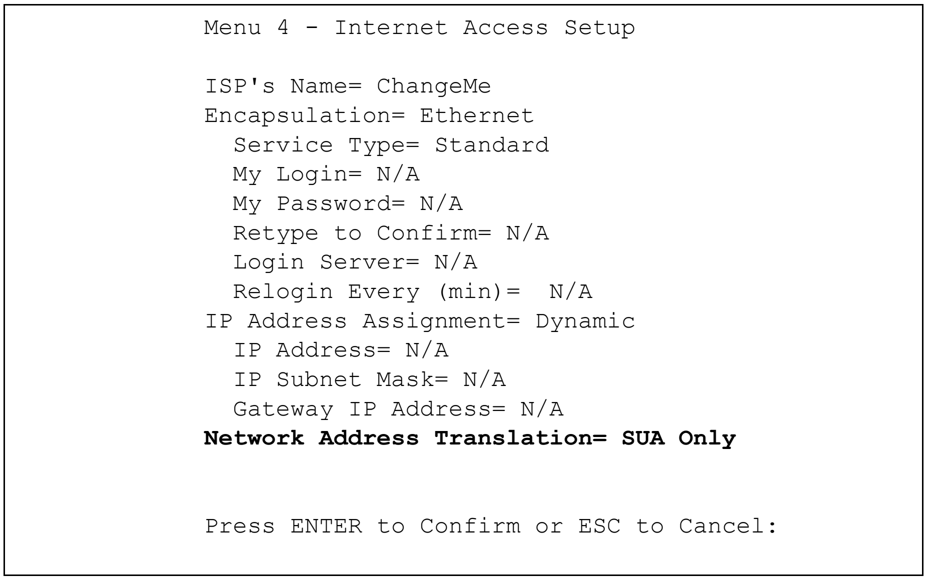
Choose SUA Only if you have just one public WAN IP address for your ZyWALL.

Choose Full Feature if you have multiple public WAN IP addresses for your ZyWALL.

### 36.1.2 Applying NAT

You apply NAT via menus 4 or 11.1.2 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

**Figure 341** Menu 4: Applying NAT for Internet Access

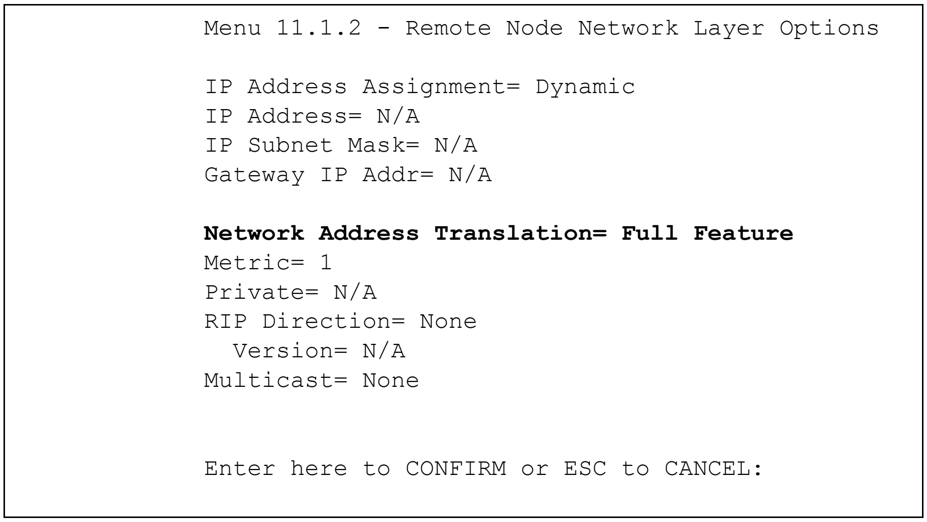


```
              Menu 4 - Internet Access Setup

              ISP's Name= ChangeMe
              Encapsulation= Ethernet
                Service Type= Standard
                My Login= N/A
                My Password= N/A
                Retype to Confirm= N/A
                Login Server= N/A
                Relogin Every (min)=  N/A
              IP Address Assignment= Dynamic
                IP Address= N/A
                IP Subnet Mask= N/A
                Gateway IP Address= N/A
              Network Address Translation= SUA Only


              Press ENTER to Confirm or ESC to Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.1.

1. Enter 11 from the main menu.
2. Enter 1 to open **Menu 11.1 - Remote Node Profile**.
3. Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.1.2 - Remote Node Network Layer Options**.

**Figure 342** Menu 11.1.2: Applying NAT to the Remote Node



```
              Menu 11.1.2 - Remote Node Network Layer Options

              IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Addr= N/A

              Network Address Translation= Full Feature
              Metric= 1
              Private= N/A
              RIP Direction= None
                Version= N/A
              Multicast= None


              Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

**Table 196** Applying NAT in Menus 4 & 11.1.2

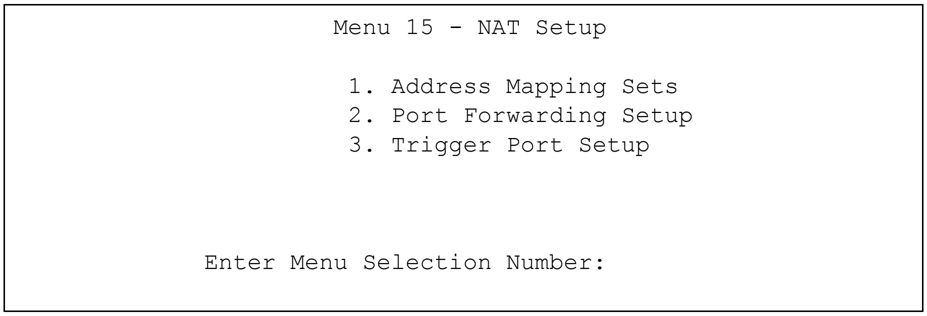
| FIELD | DESCRIPTION | OPTIONS |
|---|---|---|
| Network Address Translation | When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see Section 36.2.1 on page 523 for further discussion). You can configure any of the mapping types described in Chapter 17 on page 331. Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL.<br>When you select **Full Feature** you must configure at least one address mapping set. | Full Feature |
| | NAT is disabled when you select this option. | None |
| | When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see Section 36.2.1 on page 523). Choose **SUA Only** if you have just one public WAN IP address for your ZyWALL. | SUA Only |

## 36.2 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN, WLAN and DMZ. **Set 255** is used for SUA. When you select **Full Feature** in menu 4, menu 11.1.2, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN, WLAN and DMZ servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in Chapter 17 on page 331 for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

**Figure 343** Menu 15: NAT Setup



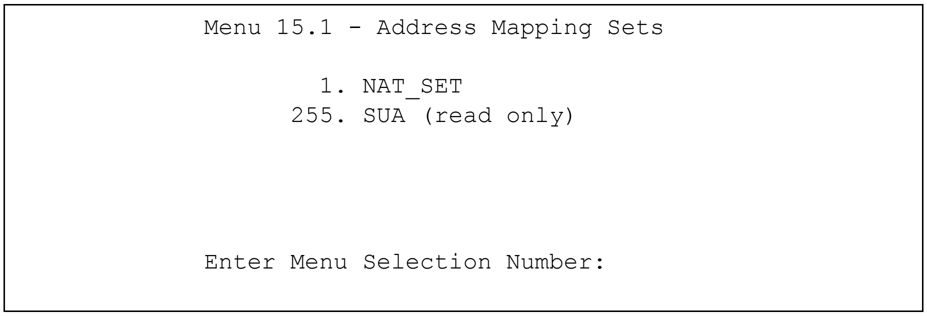
```
                               Menu 15 - NAT Setup

                                1. Address Mapping Sets
                                2. Port Forwarding Setup
                                3. Trigger Port Setup



                      Enter Menu Selection Number:
```

Configure DMZ, WLAN and LAN IP addresses in NAT menus 15.1 and 15.2. DMZ, WLAN and LAN IP addresses must be on separate subnets.

### 36.2.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 - Address Mapping Sets**.

**Figure 344** Menu 15.1: Address Mapping Sets

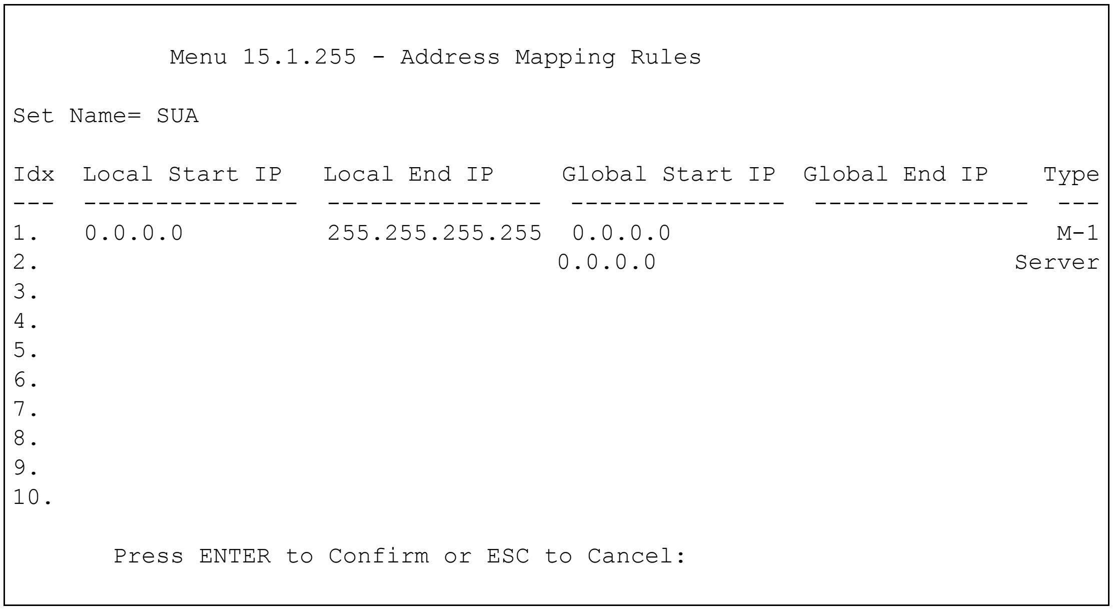


```
             Menu 15.1 - Address Mapping Sets

                     1. NAT_SET
                   255. SUA (read only)




             Enter Menu Selection Number:
```

### 36.2.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also Section 36.1.1 on page 521). The fields in this menu cannot be changed.

**Figure 345** Menu 15.1.255: SUA Address Mapping Rules



```
           Menu 15.1.255 - Address Mapping Rules

Set Name= SUA

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------   ---
1.   0.0.0.0          255.255.255.255  0.0.0.0                            M-1
2.                                    0.0.0.0                          Server
3.
4.
5.
6.
7.
8.
9.
10.

       Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

Menu 15.1.255 is read-only.

**Table 197** SUA Address Mapping Rules

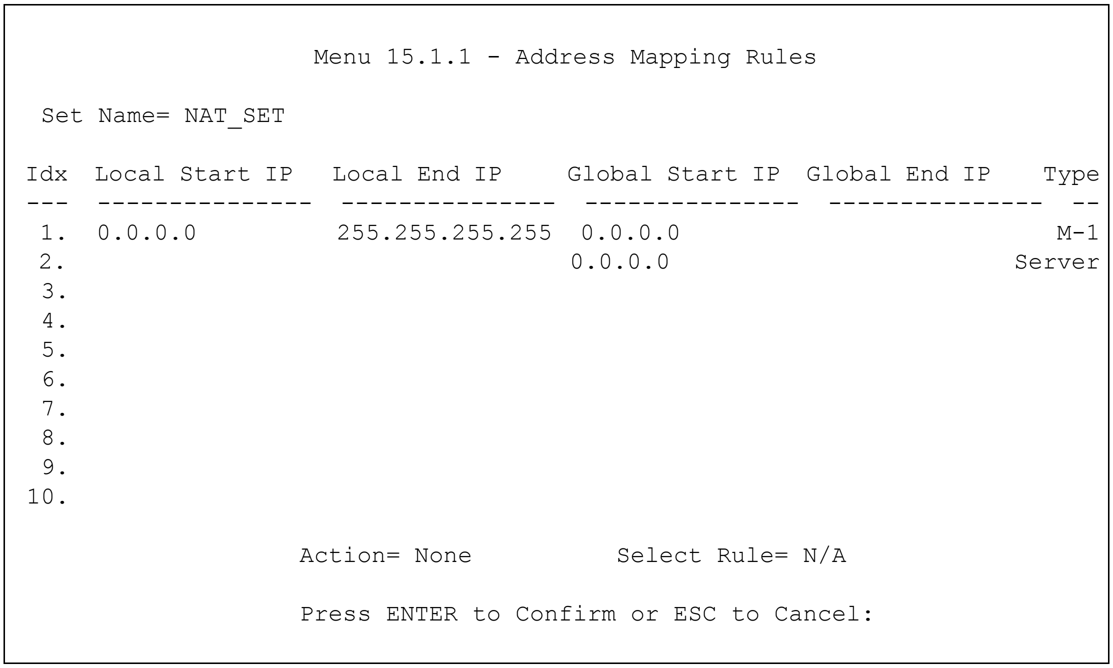
| FIELD | DESCRIPTION |
|---|---|
| Set Name | This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create. |
| Idx | This is the index or rule number. |
| Local Start IP | **Local Start IP** is the starting local IP address (ILA). |
| Local End IP | **Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the start IP is 0.0.0.0 and the end IP is 255.255.255.255. |
| Global Start IP | This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**. |
| Global End IP | This is the ending global IP address (IGA). |
| Type | These are the mapping types discussed above. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples. |
| Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel. | |

### 36.2.1.2 User-Defined Address Mapping Sets

Now look at option 1 in menu 15.1. Enter 1 to bring up this menu. Look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

The entire set will be deleted if you leave the **Set Name** field blank and press [ENTER] at the bottom of the screen.

**Figure 346** Menu 15.1.1: First Set



```
                  Menu 15.1.1 - Address Mapping Rules

 Set Name= NAT_SET

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  --
 1.  0.0.0.0          255.255.255.255  0.0.0.0                           M-1
 2.                                   0.0.0.0                         Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                   Action= None          Select Rule= N/A

                   Press ENTER to Confirm or ESC to Cancel:
```

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

### 36.2.1.3 Ordering Your Rules

Ordering your rules is important because the ZyWALL applies the rules in the order that you specify. When a rule matches the current packet, the ZyWALL takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

**Table 198** Fields in Menu 15.1.1

| FIELD | DESCRIPTION |
|---|---|
| Set Name | Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted. |
| Action | The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item. |
| Select Rule | When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question. |

---

You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

---

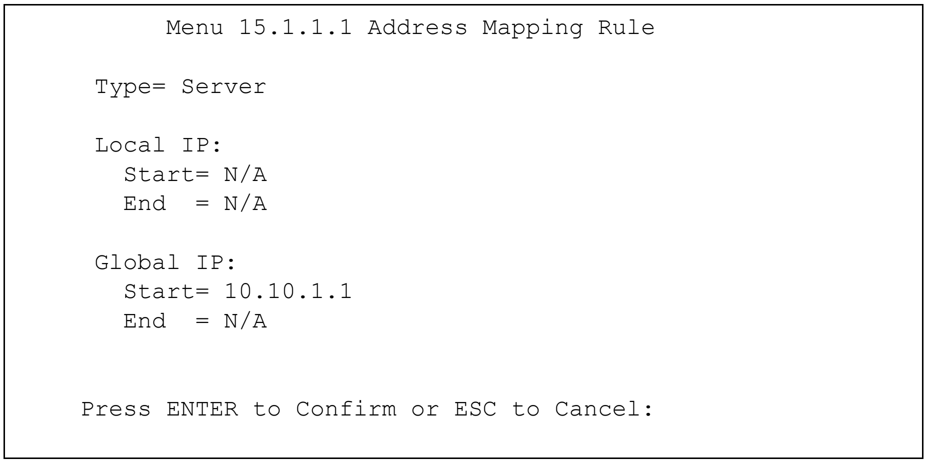
Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

---

An IP End address must be numerically greater than its corresponding IP Start address.

---

**Figure 347** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set



```
           Menu 15.1.1.1 Address Mapping Rule

      Type= Server

      Local IP:
        Start= N/A
        End   = N/A

      Global IP:
        Start= 10.10.1.1
        End   = N/A


     Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 199** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

| FIELD | DESCRIPTION |
|---|---|
| Type | Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in Chapter 17 on page 331. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See Section 36.4.3 on page 532 for an example. |
| Local IP | Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**. |
| Start | Enter the starting local IP address (ILA). |
| End | Enter the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types. |
| Global IP | |

**Table 199** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

| FIELD | DESCRIPTION |
|---|---|
| Start | Enter the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**. |
| End | Enter the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**. |
| Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel. | |

## 36.3 Configuring a Server behind NAT

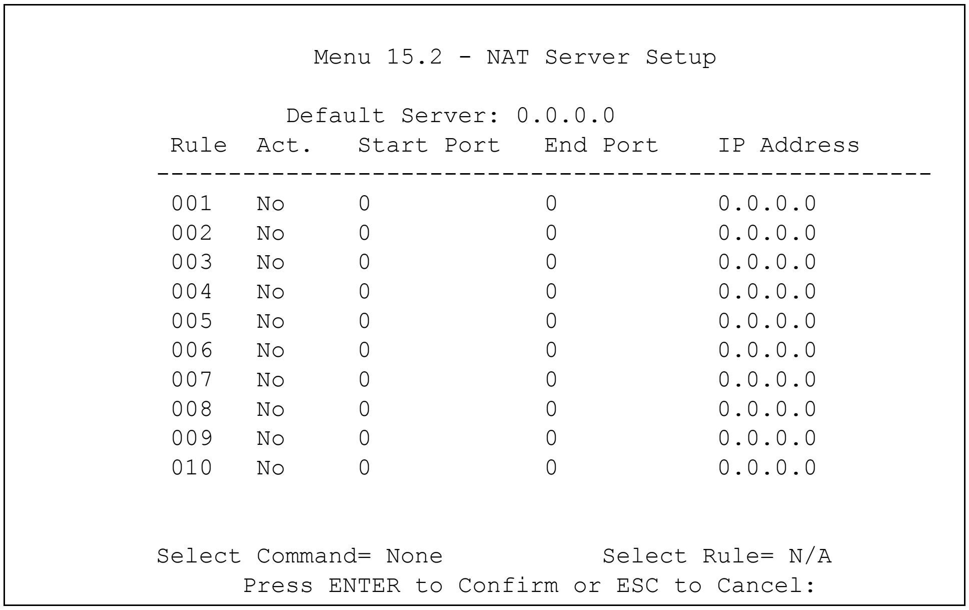
If you do not assign a Default Server IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

Follow these steps to configure a server behind NAT:

1 Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.

2 Enter 2 to open menu 15.2 and configure the address mapping rules for the WAN port.

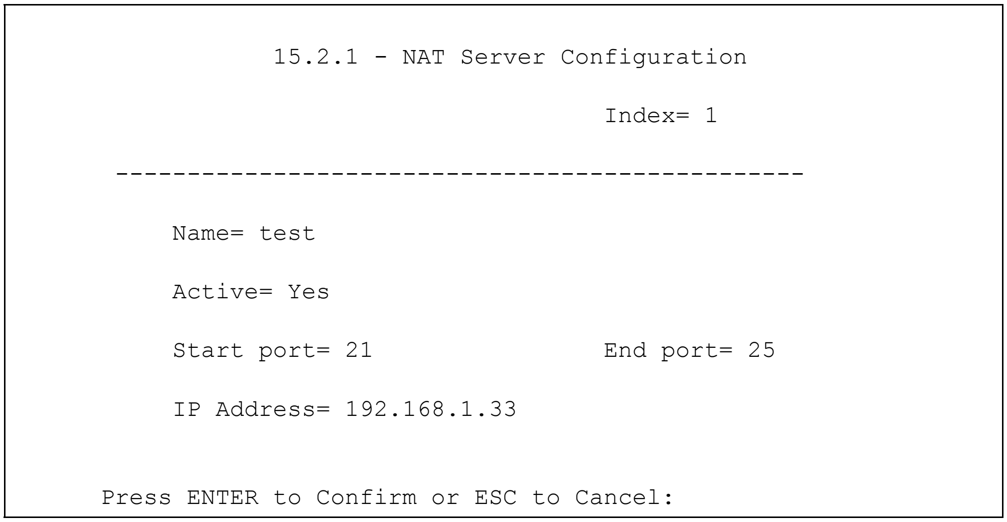
**Figure 348** Menu 15.2: NAT Server Sets



```
                    Menu 15.2 - NAT Server Setup

                  Default Server: 0.0.0.0
          Rule  Act.   Start Port   End Port    IP Address
         ------------------------------------------------------
          001   No     0            0           0.0.0.0
          002   No     0            0           0.0.0.0
          003   No     0            0           0.0.0.0
          004   No     0            0           0.0.0.0
          005   No     0            0           0.0.0.0
          006   No     0            0           0.0.0.0
          007   No     0            0           0.0.0.0
          008   No     0            0           0.0.0.0
          009   No     0            0           0.0.0.0
          010   No     0            0           0.0.0.0


         Select Command= None           Select Rule= N/A
               Press ENTER to Confirm or ESC to Cancel:
```

3 Select **Edit Rule** in the **Select Command** field; type the index number of the NAT server you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 15.2.x - NAT Server Configuration** (see the next figure).

**Figure 349** 15.2.1: NAT Server Configuration



```
                   15.2.1 - NAT Server Configuration

                                              Index= 1

        ------------------------------------------------

            Name= test

            Active= Yes

            Start port= 21                End port= 25

            IP Address= 192.168.1.33


       Press ENTER to Confirm or ESC to Cancel:
```

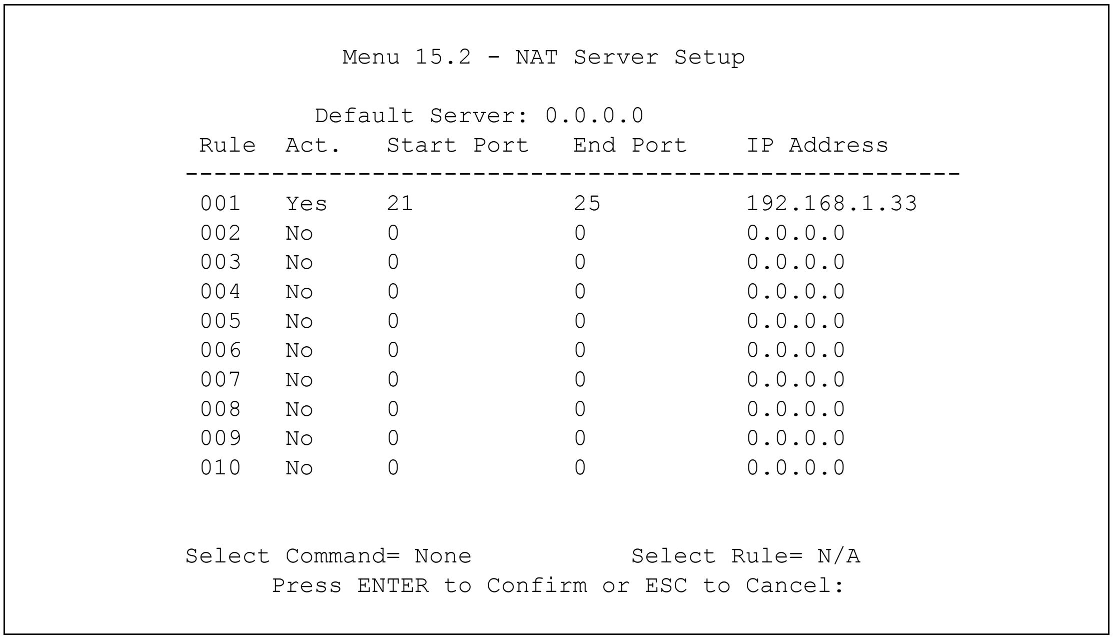
The following table describes the fields in this screen.

**Table 200** 15.2.1: NAT Server Configuration

| FIELD | DESCRIPTION |
|---|---|
| Index | This is the index number of an individual port forwarding server entry. |
| Name | Enter a name to identify this port-forwarding rule. |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the NAT server entry. |
| Start Port<br>End Port | Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field. |
| IP Address | Enter the inside IP address of the server. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

4. Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.
5. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
6. Press [ENTER] at the “Press ENTER to confirm …” prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

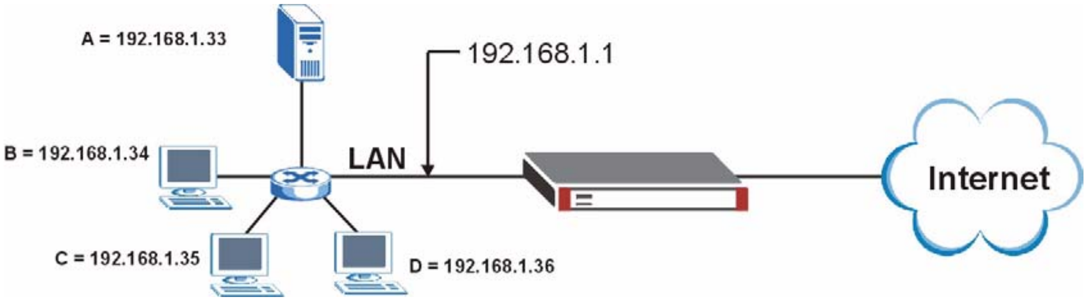
**Figure 350** Menu 15.2: NAT Server Setup



```
                    Menu 15.2 - NAT Server Setup

                  Default Server: 0.0.0.0
          Rule   Act.   Start Port   End Port    IP Address
         ------------------------------------------------------
          001    Yes     21           25          192.168.1.33
          002    No      0            0           0.0.0.0
          003    No      0            0           0.0.0.0
          004    No      0            0           0.0.0.0
          005    No      0            0           0.0.0.0
          006    No      0            0           0.0.0.0
          007    No      0            0           0.0.0.0
          008    No      0            0           0.0.0.0
          009    No      0            0           0.0.0.0
          010    No      0            0           0.0.0.0


         Select Command= None           Select Rule= N/A
               Press ENTER to Confirm or ESC to Cancel:
```

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. **A** is the FTP/Telnet/SMTP server.

**Figure 351** Server Behind NAT Example



## 36.4 General NAT Examples

The following are some examples of NAT configuration.

### 36.4.1 Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

**Figure 352** NAT Example 1

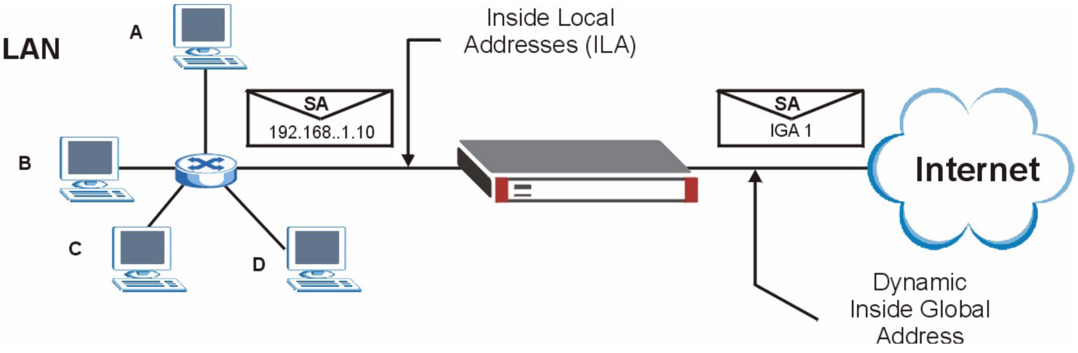
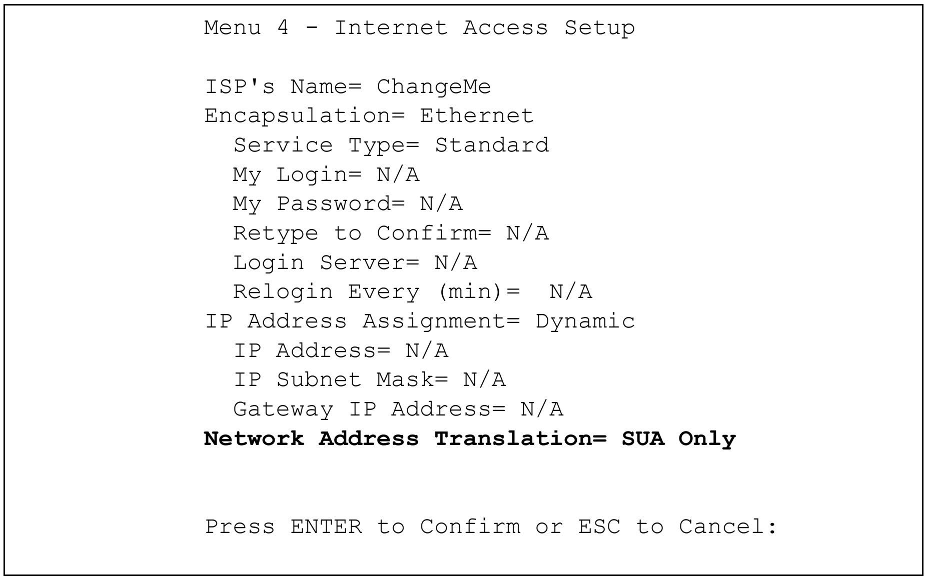

LAN
A
B
C
D
SA
192.168..1.10
Inside Local
Addresses (ILA)
SA
IGA 1
Internet
Dynamic
Inside Global
Address

**Figure 353** Menu 4: Internet Access & NAT Example

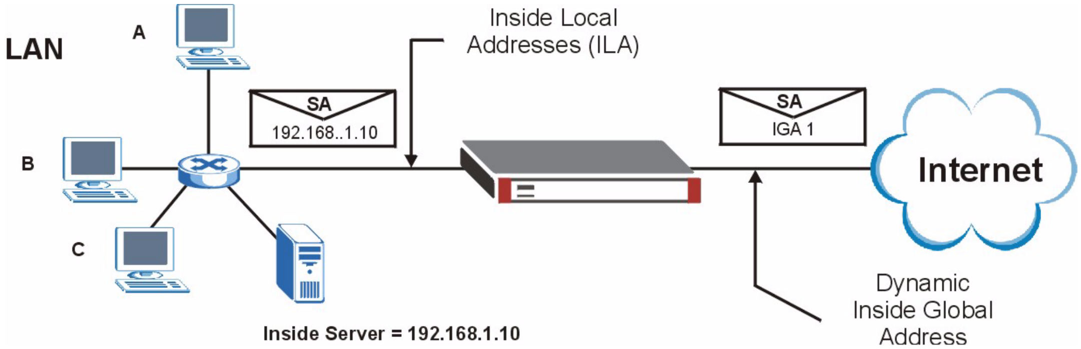


```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Retype to Confirm= N/A
  Login Server= N/A
  Relogin Every (min)=  N/A
IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only


Press ENTER to Confirm or ESC to Cancel:
```

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in Section 36.4 on page 530. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.1.2 is specifically pre-configured to handle this case.

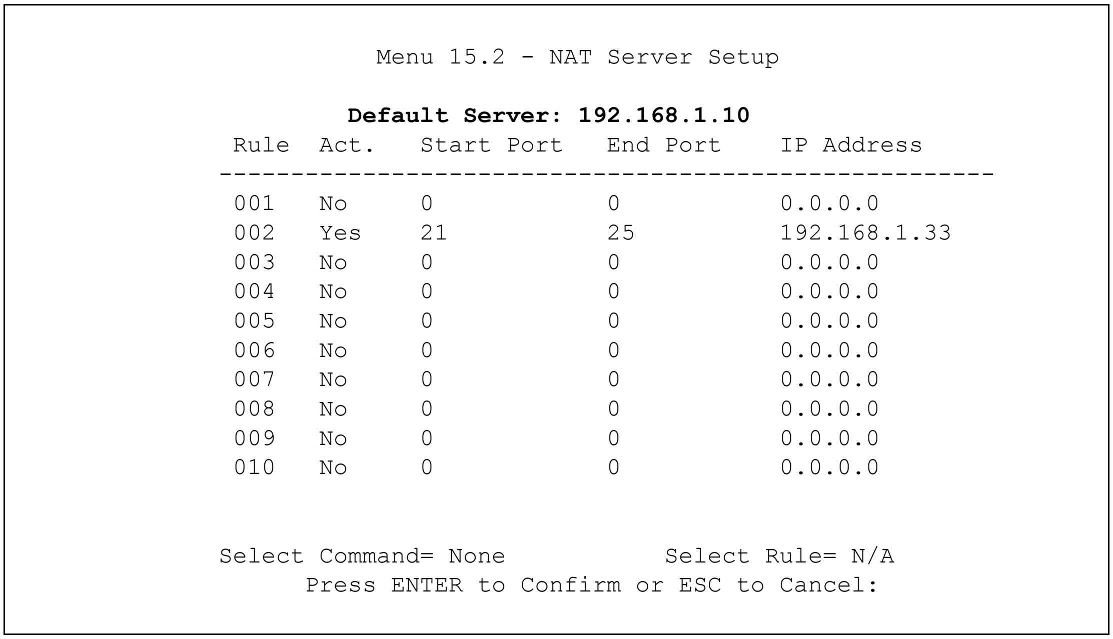
## 36.4.2 Example 2: Internet Access with a Default Server

**Figure 354** NAT Example 2


LAN
A
B
C
SA
192.168..1.10
Inside Local Addresses (ILA)
SA
IGA 1
Internet
Dynamic Inside Global Address
Inside Server = 192.168.1.10

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the **Default Server** behind the NAT as shown in the next figure.

**Figure 355** Menu 15.2: Specifying an Inside Server



```
                    Menu 15.2 - NAT Server Setup

                  Default Server: 192.168.1.10
          Rule  Act.    Start Port   End Port     IP Address
         ------------------------------------------------------
          001   No      0            0            0.0.0.0
          002   Yes     21           25           192.168.1.33
          003   No      0            0            0.0.0.0
          004   No      0            0            0.0.0.0
          005   No      0            0            0.0.0.0
          006   No      0            0            0.0.0.0
          007   No      0            0            0.0.0.0
          008   No      0            0            0.0.0.0
          009   No      0            0            0.0.0.0
          010   No      0            0            0.0.0.0


         Select Command= None            Select Rule= N/A
               Press ENTER to Confirm or ESC to Cancel:
```

## 36.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

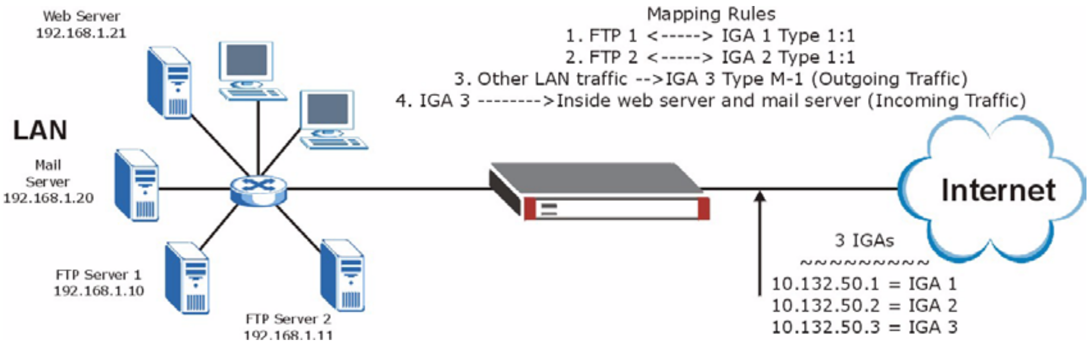
In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

1 Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

**Figure 356** NAT Example 3


Web Server
192.168.1.21
Mapping Rules
1. FTP 1 <-----> IGA 1 Type 1:1
2. FTP 2 <-----> IGA 2 Type 1:1
3. Other LAN traffic -->IGA 3 Type M-1 (Outgoing Traffic)
4. IGA 3 -------->Inside web server and mail server (Incoming Traffic)
LAN
Mail
Server
192.168.1.20
Internet
3 IGAs
~~~~~~~~~~
10.132.50.1 = IGA 1
10.132.50.2 = IGA 2
10.132.50.3 = IGA 3
FTP Server 1
192.168.1.10
FTP Server 2
192.168.1.11

1. In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in Figure 357 on page 534.
2. Then enter 15 from the main menu.
3. Enter 1 to configure the Address Mapping Sets.
4. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
5. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See Figure 358 on page 534*)*.
6. Repeat the previous step for rules 2 to 4 as outlined above.
7. When finished, menu 15.1.1 should look like as shown in Figure 359 on page 535.
~~~~~~~~~~

**Figure 357** Example 3: Menu 11.1.2

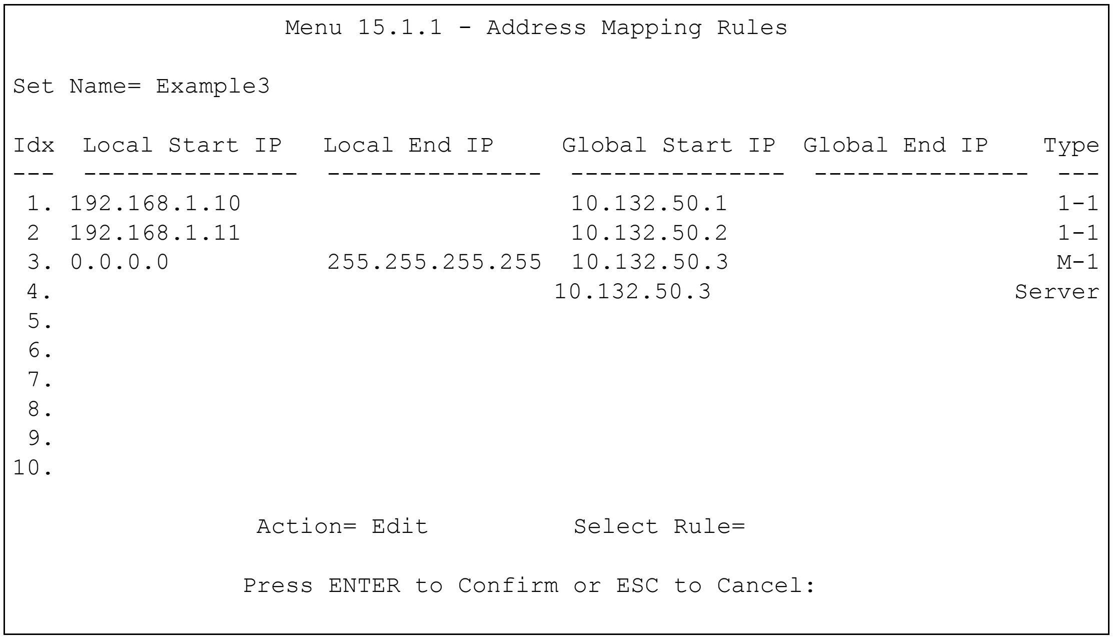
```
              Menu 11.1.2 - Remote Node Network Layer Options

                       IP Address Assignment= Dynamic
                       IP Address= N/A
                       IP Subnet Mask= N/A
                       Gateway IP Addr= N/A

                       Network Address Translation= SUA Only
                       Metric= 2
                       Private=
                       RIP Direction= None
                         Version= N/A
                       Multicast= None


               Enter here to CONFIRM or ESC to CANCEL:
```

The following figure shows how to configure the first rule.

**Figure 358** Example 3: Menu 15.1.1.1

```
              Menu 15.1.1.1 Address Mapping Rule

                  Type= One-to-One

                  Local IP:
                    Start= 192.168.1.10
                    End  = N/A

                  Global IP:
                    Start= 10.132.50.1
                    End  = N/A

              Press ENTER to Confirm or ESC to Cancel:
```

**Figure 359** Example 3: Final Menu 15.1.1

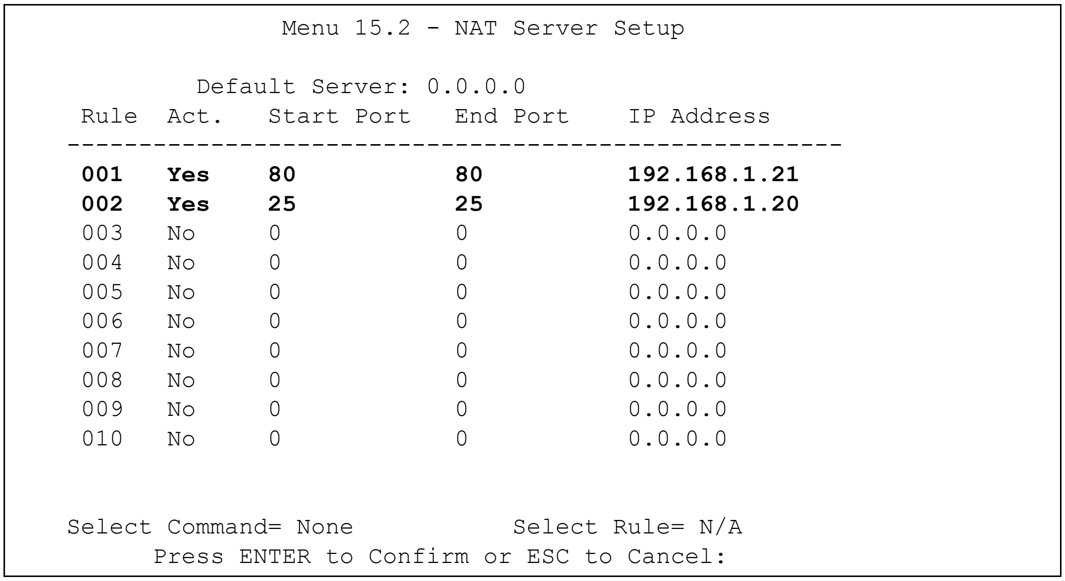


```
                    Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ---
 1. 192.168.1.10                        10.132.50.1                      1-1
 2  192.168.1.11                        10.132.50.2                      1-1
 3. 0.0.0.0          255.255.255.255  10.132.50.3                      M-1
 4.                                    10.132.50.3                     Server
 5.
 6.
 7.
 8.
 9.
10.

                  Action= Edit          Select Rule=

                 Press ENTER to Confirm or ESC to Cancel:
```

Now configure the IGA3 to map to our web server and mail server on the LAN.

1. Enter 15 from the main menu.
2. Enter 2 to go to menu 15.2 and configure it as shown in Figure 360 on page 535.

**Figure 360** Example 3: Menu 15.2.

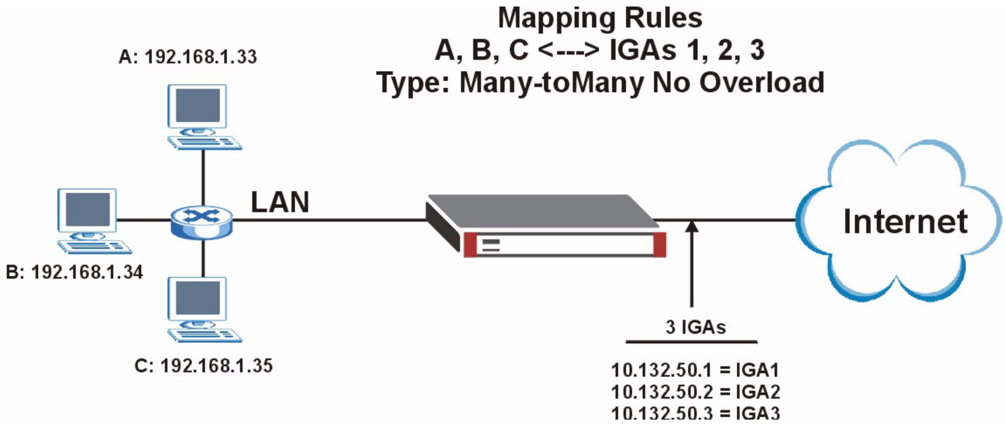


```
                   Menu 15.2 - NAT Server Setup

             Default Server: 0.0.0.0
     Rule  Act.   Start Port   End Port    IP Address
    ------------------------------------------------------
     001   Yes    80           80          192.168.1.21
     002   Yes    25           25          192.168.1.20
     003   No     0            0           0.0.0.0
     004   No     0            0           0.0.0.0
     005   No     0            0           0.0.0.0
     006   No     0            0           0.0.0.0
     007   No     0            0           0.0.0.0
     008   No     0            0           0.0.0.0
     009   No     0            0           0.0.0.0
     010   No     0            0           0.0.0.0


    Select Command= None           Select Rule= N/A
          Press ENTER to Confirm or ESC to Cancel:
```

## 36.4.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-One-to-One** mapping as port numbers do *not* change for **Many-One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

**Figure 361** NAT Example 4


Mapping Rules
A, B, C <---> IGAs 1, 2, 3
Type: Many-toMany No Overload
A: 192.168.1.33
B: 192.168.1.34
C: 192.168.1.35
LAN
Internet
3 IGAs
10.132.50.1 = IGA1
10.132.50.2 = IGA2
10.132.50.3 = IGA3

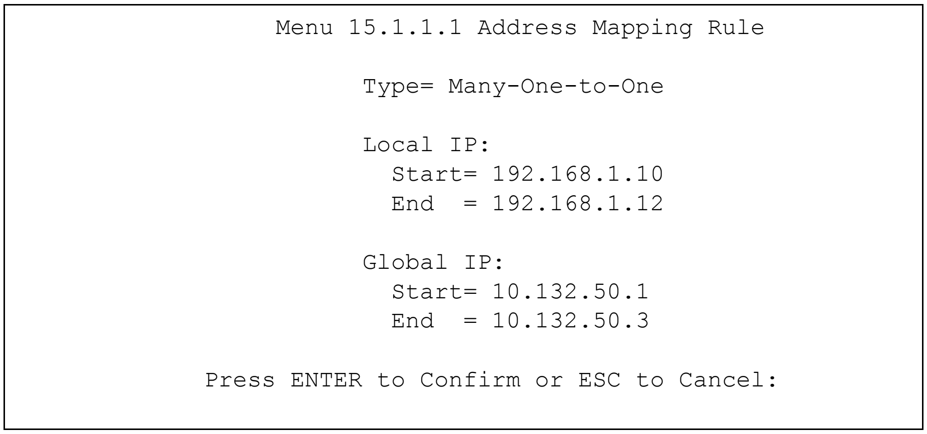
---

Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won’t work through NAT even when using One-to-One and Many-One-to-One mapping types.

---

Follow the steps outlined in example 3 above to configure these two menus as follows.

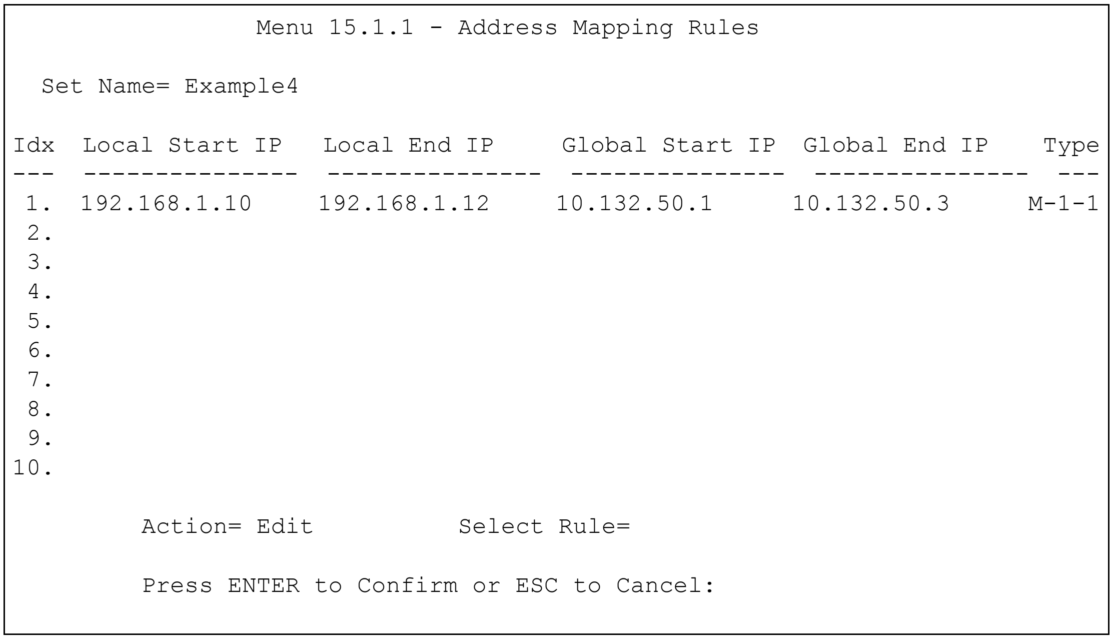
**Figure 362** Example 4: Menu 15.1.1.1: Address Mapping Rule



```
     Menu 15.1.1.1 Address Mapping Rule

           Type= Many-One-to-One

           Local IP:
             Start= 192.168.1.10
             End  = 192.168.1.12

           Global IP:
             Start= 10.132.50.1
             End  = 10.132.50.3

Press ENTER to Confirm or ESC to Cancel:
```

After you’ve configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

**Figure 363** Example 4: Menu 15.1.1: Address Mapping Rules



```
                Menu 15.1.1 - Address Mapping Rules

  Set Name= Example4

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ---
 1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3     M-1-1
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

         Action= Edit          Select Rule=

         Press ENTER to Confirm or ESC to Cancel:
```

## 36.5 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

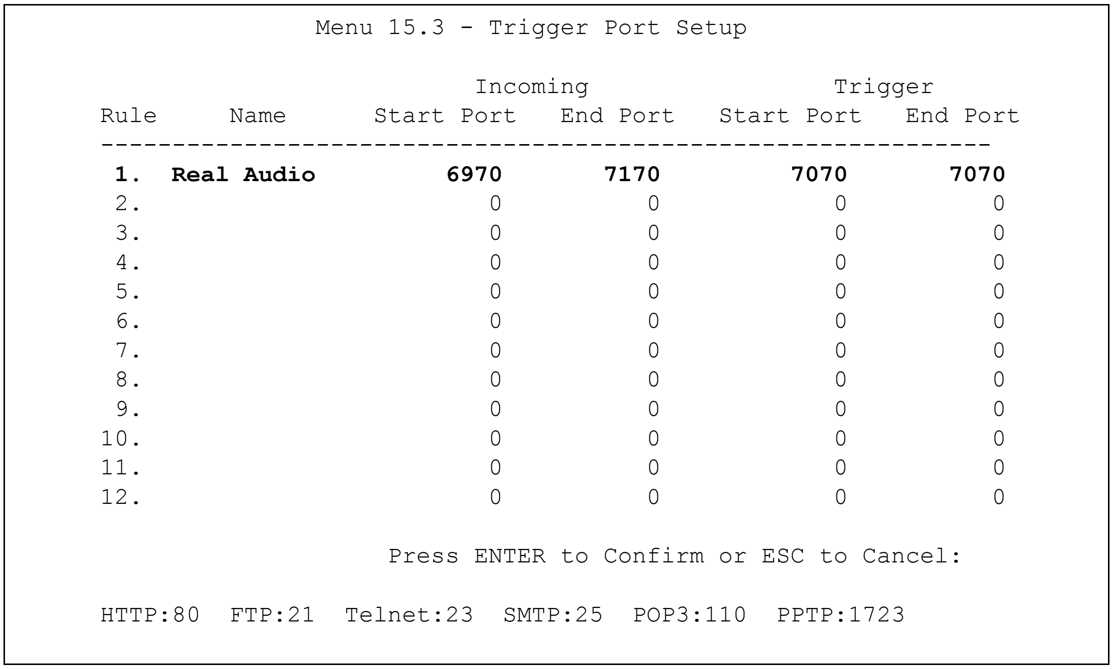
### 36.5.1 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is going coming from inside the ZyWALL and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it.

Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 - Trigger Port Setup** and configure trigger port rules for the WAN port.

**Figure 364** Menu 15.3.1: Trigger Port Setup



```
                    Menu 15.3 - Trigger Port Setup

                               Incoming                 Trigger
      Rule     Name      Start Port   End Port   Start Port   End Port
      --------------------------------------------------------------
       1.  Real Audio         6970       7170         7070       7070
       2.                        0          0            0          0
       3.                        0          0            0          0
       4.                        0          0            0          0
       5.                        0          0            0          0
       6.                        0          0            0          0
       7.                        0          0            0          0
       8.                        0          0            0          0
       9.                        0          0            0          0
      10.                        0          0            0          0
      11.                        0          0            0          0
      12.                        0          0            0          0

                          Press ENTER to Confirm or ESC to Cancel:

      HTTP:80  FTP:21  Telnet:23  SMTP:25  POP3:110  PPTP:1723
```

The following table describes the fields in this menu.

**Table 201** Menu 15.3: Trigger Port Setup

| FIELD | DESCRIPTION |
|---|---|
| Rule | This is the rule index number. |
| Name | Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces. |
| Incoming | Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. |
| Start Port | Enter a port number or the starting port number in a range of port numbers. |
| End Port | Enter a port number or the ending port number in a range of port numbers. |
| Trigger | The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN. |
| Start Port | Enter a port number or the starting port number in a range of port numbers. |
| End Port | Enter a port number or the ending port number in a range of port numbers. |
| Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel. | |

# 37

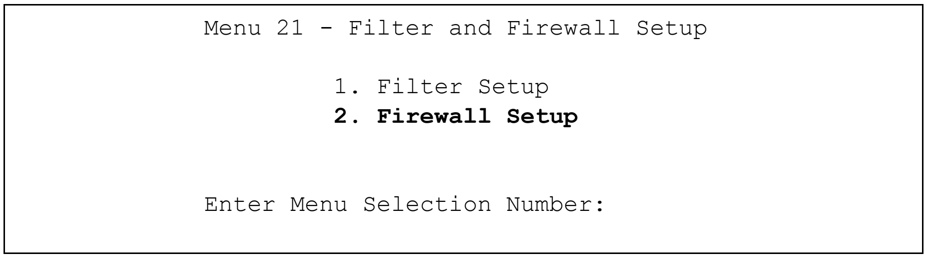
# Introducing the ZyWALL Firewall

This chapter shows you how to get started with the ZyWALL firewall.

## 37.1 Using ZyWALL SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next.

**Figure 365** Menu 21: Filter and Firewall Setup

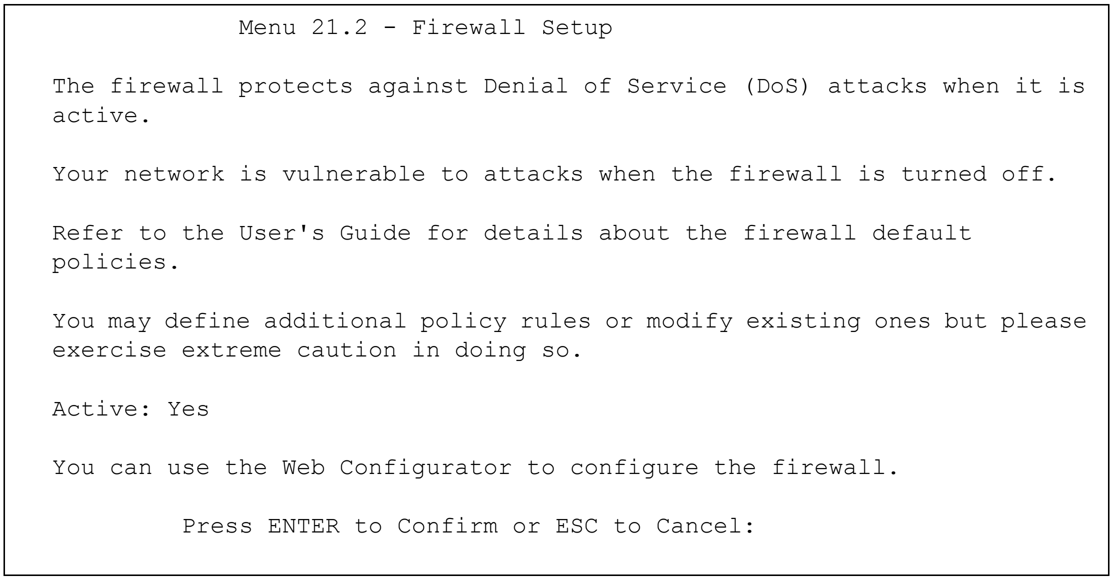


```
                  Menu 21 - Filter and Firewall Setup

                           1. Filter Setup
                           2. Firewall Setup


                  Enter Menu Selection Number:
```

### 37.1.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Use the web configurator to configure firewall rules.

**Figure 366** Menu 21.2: Firewall Setup



```
                Menu 21.2 - Firewall Setup

   The firewall protects against Denial of Service (DoS) attacks when it is
   active.

   Your network is vulnerable to attacks when the firewall is turned off.

   Refer to the User's Guide for details about the firewall default
   policies.

   You may define additional policy rules or modify existing ones but please
   exercise extreme caution in doing so.

   Active: Yes

   You can use the Web Configurator to configure the firewall.

            Press ENTER to Confirm or ESC to Cancel:
```

Configure the firewall rules using the web configurator or CLI commands.

# 38

# Filter Configuration

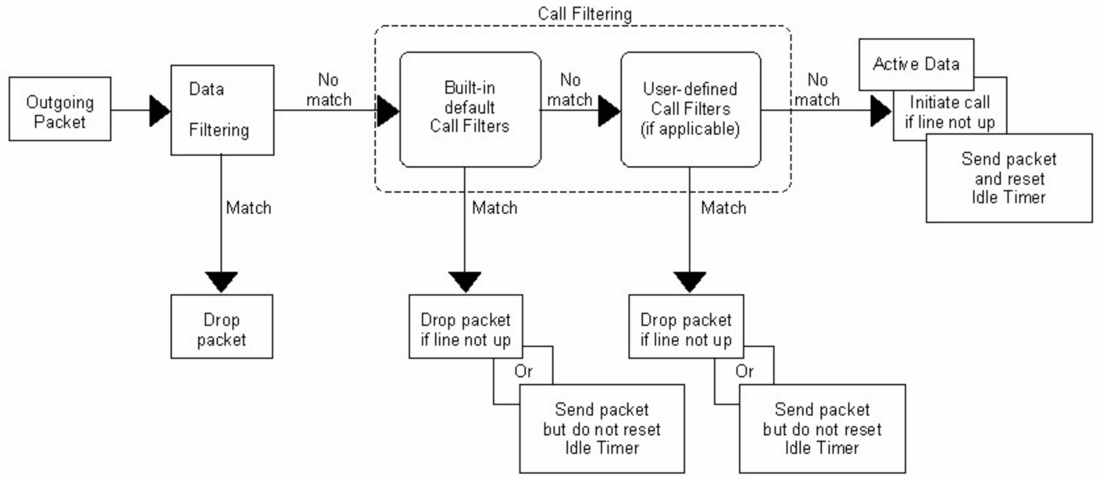
This chapter shows you how to create and apply filters.

## 38.1 Introduction to Filters

Your ZyWALL uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

**Figure 367** Outgoing Packet Filtering Process


Call Filtering
Outgoing Packet
Data Filtering
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset Idle Timer
Drop packet if line not up
Or
Send packet but do not reset Idle Timer

For incoming packets, your ZyWALL applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

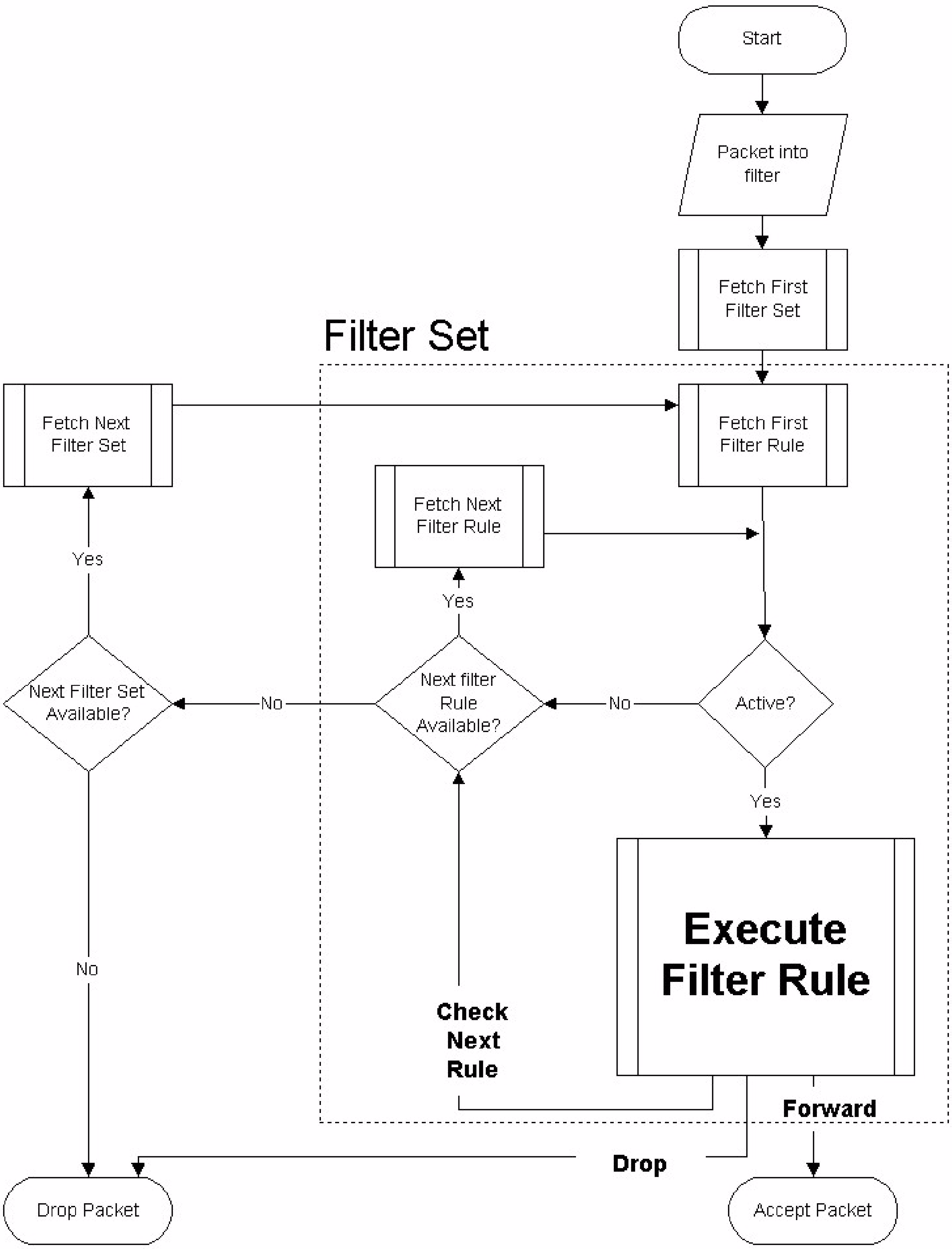
### 38.1.1 The Filter Structure of the ZyWALL

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The ZyWALL allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming Telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also Figure 373 on page 548 for the logic flow when executing an IP filter.

**Figure 368** Filter Rule Process


Start
Packet into filter
Fetch First Filter Set
Filter Set
Fetch Next Filter Set
Fetch First Filter Rule
Fetch Next Filter Rule
Yes
Yes
Next Filter Set Available?
No
Next filter Rule Available?
No
Active?
Yes
Execute Filter Rule
No
Check Next Rule
Forward
Drop
Drop Packet
Accept Packet

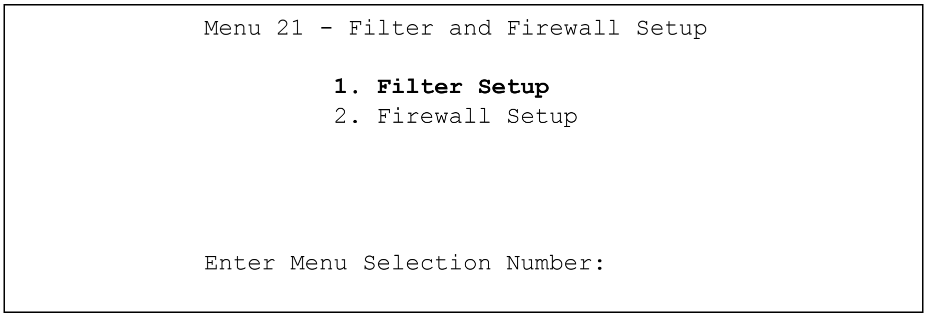
You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

## 38.2 Configuring a Filter Set

The ZyWALL includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

**1** Enter 21 in the main menu to open menu 21.

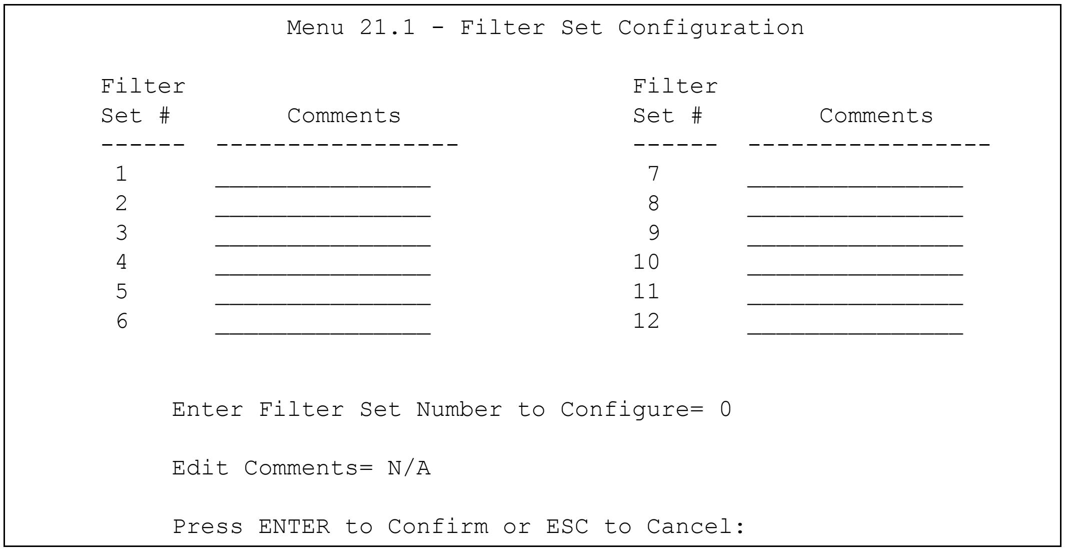
**Figure 369** Menu 21: Filter and Firewall Setup



```
              Menu 21 - Filter and Firewall Setup

                       1. Filter Setup
                       2. Firewall Setup





              Enter Menu Selection Number:
```

**2** Enter 1 to bring up the following menu.

**Figure 370** Menu 21.1: Filter Set Configuration



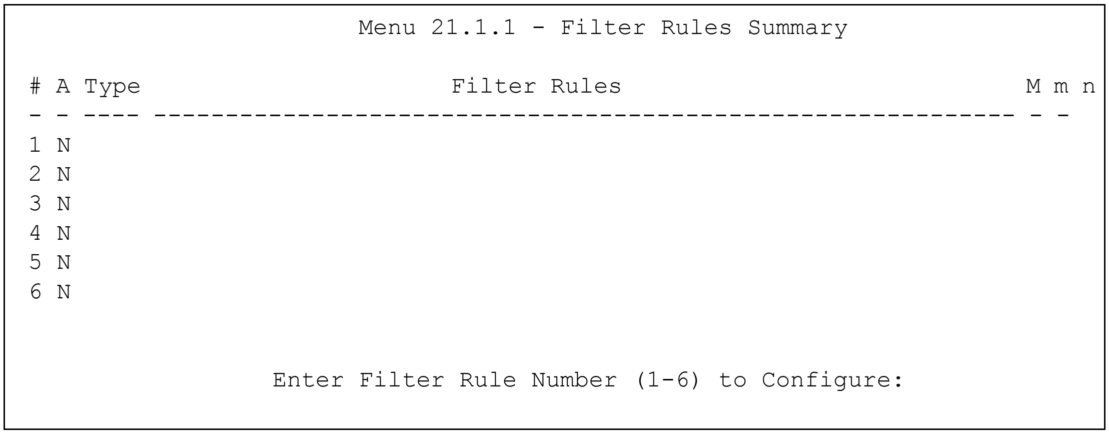
```
                    Menu 21.1 - Filter Set Configuration

      Filter                                Filter
      Set #       Comments                  Set #       Comments
      ------  -----------------             ------  -----------------
       1      _______________                7      _______________
       2      _______________                8      _______________
       3      _______________                9      _______________
       4      _______________               10      _______________
       5      _______________               11      _______________
       6      _______________               12      _______________


           Enter Filter Set Number to Configure= 0

           Edit Comments= N/A

           Press ENTER to Confirm or ESC to Cancel:
```

**3** Select the filter set you wish to configure (1-12) and press [ENTER].

**4** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

**5** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

**Figure 371** Menu 21.1.1: Filter Rules Summary



```
                         Menu 21.1.1 - Filter Rules Summary

 # A Type                      Filter Rules                             M m n
 - - ---- ------------------------------------------------------------ - -
 1 N
 2 N
 3 N
 4 N
 5 N
 6 N


                   Enter Filter Rule Number (1-6) to Configure:
```

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

**Table 202** Abbreviations Used in the Filter Rules Summary Menu

| FIELD | DESCRIPTION |
|---|---|
| A | Active: “Y” means the rule is active. “N” means the rule is inactive. |
| Type | The type of filter rule: “GEN” for Generic, “IP” for TCP/IP. |
| Filter Rules | These parameters are displayed here. |
| M | More.<br>“Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete.<br>“N” means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. |
| m | Action Matched.<br>“F” means to forward the packet immediately and skip checking the remaining rules.<br>“D” means to drop the packet.<br>“N“ means to check the next rule. |
| n | Action Not Matched.<br>“F” means to forward the packet immediately and skip checking the remaining rules.<br>“D” means to drop the packet.<br>“N” means to check the next rule. |

The protocol dependent filter rules abbreviation are listed as follows:

**Table 203** Rule Abbreviations Used

| ABBREVIATION | DESCRIPTION |
|---|---|
| IP | |
| Pr | Protocol |
| SA | Source Address |
| SP | Source Port number |
| DA | Destination Address |
| DP | Destination Port number |
| GEN | |

**Table 203** Rule Abbreviations Used

| ABBREVIATION | DESCRIPTION |
|---|---|
| Off | Offset |
| Len | Length |

Refer to the next section for information on configuring the filter rules.

## 38.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

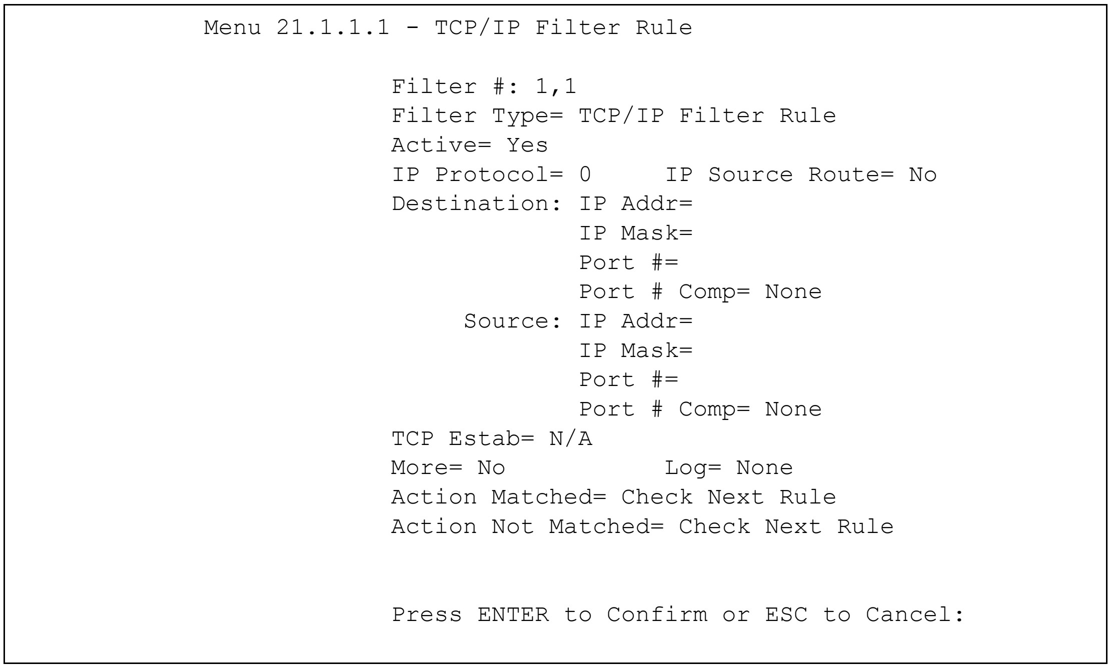
To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the ZyWALL will warn you and will not allow you to save.

## 38.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next.

**Figure 372** Menu 21.1.1.1: TCP/IP Filter Rule



```
              Menu 21.1.1.1 - TCP/IP Filter Rule

                           Filter #: 1,1
                           Filter Type= TCP/IP Filter Rule
                           Active= Yes
                           IP Protocol= 0     IP Source Route= No
                           Destination: IP Addr=
                                        IP Mask=
                                        Port #=
                                        Port # Comp= None
                                Source: IP Addr=
                                        IP Mask=
                                        Port #=
                                        Port # Comp= None
                           TCP Estab= N/A
                           More= No           Log= None
                           Action Matched= Check Next Rule
                           Action Not Matched= Check Next Rule


                           Press ENTER to Confirm or ESC to Cancel:
```

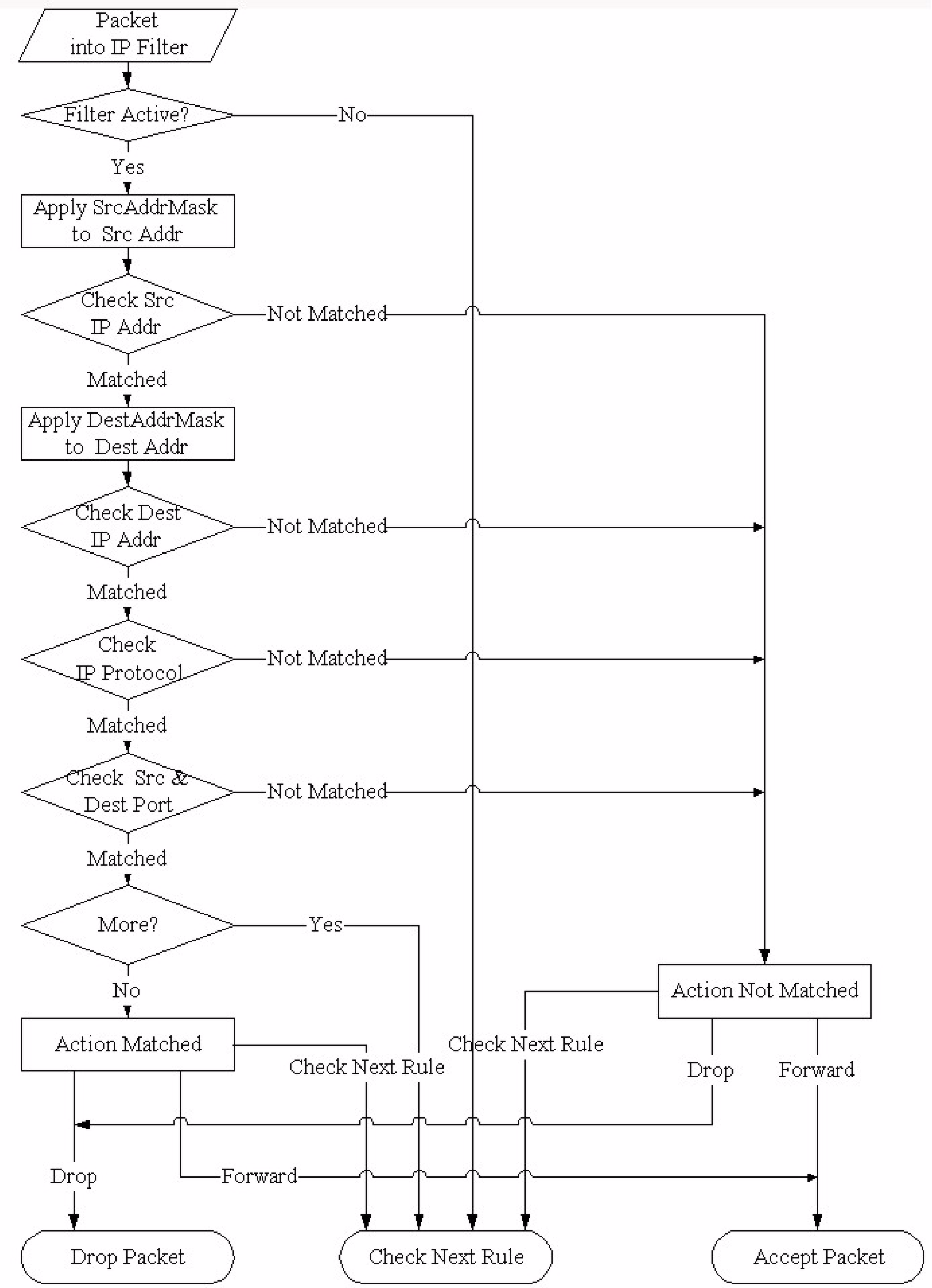
The following table describes how to configure your TCP/IP filter rule.

**Table 204** Menu 21.1.1.1: TCP/IP Filter Rule

| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the filter rule or **No** to deactivate it. |
| IP Protocol | Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol. |
| IP Source Route | Press [SPACE BAR] and then [ENTER] to select **Yes** to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route. |
| Destination | |
| IP Addr | Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0. |
| IP Mask | Enter the IP mask to apply to the **Destination: IP Addr**. |
| Port # | Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0. |
| Port # Comp | Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #**.<br>Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**. |
| Source | |
| IP Addr | Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0. |
| IP Mask | Enter the IP mask to apply to the **Source: IP Addr**. |
| Port # | Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0. |
| Port # Comp | Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**.<br>Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**. |
| TCP Estab | This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored. |
| More | Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields.<br>If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**. |
| Log | Press [SPACE BAR] and then [ENTER] to select a logging option from the following:<br>**None** – No packets will be logged.<br>**Action Matched** - Only packets that match the rule parameters will be logged.<br>**Action Not Matched** - Only packets that do not match the rule parameters will be logged.<br>**Both** – All packets will be logged. |
| Action Matched | Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.<br>Options are **Check Next Rule**, **Forward** and **Drop**. |
| Action Not Matched | Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.<br>Options are **Check Next Rule**, **Forward** and **Drop**. |
| When you have **Menu 21.1.1.1 - TCP/IP Filter Rule** configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**. | |

The following figure illustrates the logic flow of an IP filter.

**Figure 373** Executing an IP Filter


Packet into IP Filter
Filter Active?
No
Yes
Apply SrcAddrMask to Src Addr
Check Src IP Addr
Not Matched
Matched
Apply DestAddrMask to Dest Addr
Check Dest IP Addr
Not Matched
Matched
Check IP Protocol
Not Matched
Matched
Check Src & Dest Port
Not Matched
Matched
More?
Yes
No
Action Not Matched
Action Matched
Check Next Rule
Check Next Rule
Drop
Forward
Drop
Forward
Drop Packet
Check Next Rule
Accept Packet

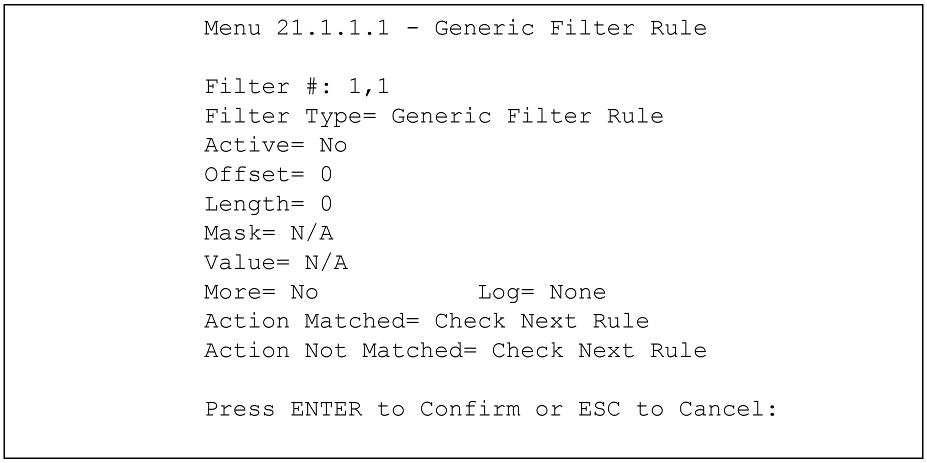
## 38.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyWALL treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyWALL applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, `FFFFFFFF`.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.1.1 and press [ENTER] to open Generic Filter Rule, as shown below.

**Figure 374** Menu 21.1.1.1: Generic Filter Rule



```
              Menu 21.1.1.1 - Generic Filter Rule

              Filter #: 1,1
              Filter Type= Generic Filter Rule
              Active= No
              Offset= 0
              Length= 0
              Mask= N/A
              Value= N/A
              More= No           Log= None
              Action Matched= Check Next Rule
              Action Not Matched= Check Next Rule

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in the **Generic Filter Rule** menu.

**Table 205** Generic Filter Rule Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| Filter # | This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set. |
| Filter Type | Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.<br>Options are **Generic Filter Rule** and **TCP/IP Filter Rule**. |
| Active | Select **Yes** to turn on the filter rule or **No** to turn it off. |
| Offset | Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255. |
| Length | Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8. |
| Mask | Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison. |
| Value | Enter the value (in Hexadecimal notation) to compare with the data portion. |

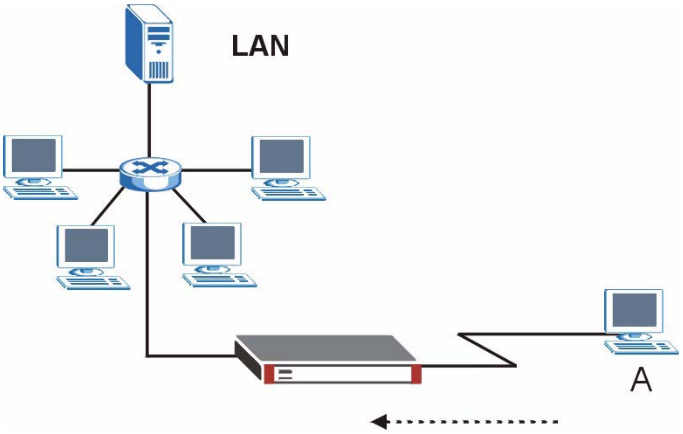
**Table 205** Generic Filter Rule Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| More | If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields.<br>If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**. |
| Log | Select the logging option from the following:<br>**None** - No packets will be logged.<br>**Action Matched** - Only packets that match the rule parameters will be logged.<br>**Action Not Matched** - Only packets that do not match the rule parameters will be logged.<br>**Both** – All packets will be logged. |
| Action Matched | Select the action for a packet matching the rule.<br>Options are **Check Next Rule**, **Forward** and **Drop**. |
| Action Not Matched | Select the action for a packet not matching the rule.<br>Options are **Check Next Rule**, **Forward** and **Drop**. |
| Once you have completed filling in **Menu 21.1.1.1 - Generic Filter Rule**, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**. | |

## 38.3 Example Filter

Let’s look at an example to block outside users from accessing the ZyWALL via Telnet. Please see our included disk for more example filters.

**Figure 375** Telnet Filter Example



1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
2 Enter 1 to open Menu 21.1 - Filter Set Configuration.
3 Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.
6 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

**Figure 376** Example Filter: Menu 21.1.3.1

```
                  Menu 21.1.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 23
             Port # Comp= Equal
     Source: IP Addr= 0.0.0.0
             IP Mask= 0.0.0.0
             Port #= 0
             Port # Comp= None
TCP Estab= No
More= No             Log= None
Action Matched= Drop
Action Not Matched= Forward

         Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

The port number for the Telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

**Figure 377** Example Filter Rules Summary: Menu 21.1.3

```
         Menu 21.1.3 - Filter Rules Summary

# A Type                      Filter Rules             M m n
- - ---- ----------------------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23             N D F
2 N
3 N
4 N
5 N
6 N


Enter Filter Rule Number (1-6) to Configure: 1
```

This shows you that you have configured and activated (**A** = **Y**) a TCP/IP filter rule (**Type** = **IP**, **Pr** = **6**) for destination Telnet ports (**DP** = **23**).

**M** = **N** means an action can be taken immediately. The action is to drop the packet (**m** = **D**) if the action is matched and to forward the packet immediately (**n** = **F**) if the action is not matched no matter whether there are more rules to be checked (there aren’t in this example).

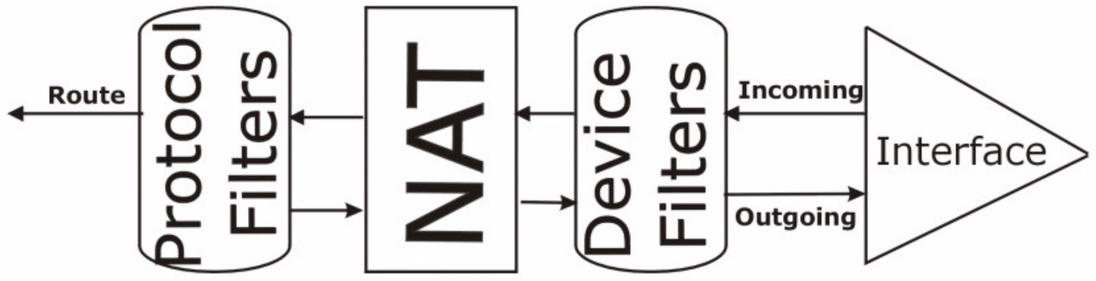
After you've created the filter set, you must apply it.

1. Enter 11 from the main menu to go to menu 11.
2. Enter 1 or 2 to open **Menu 11.x - Remote Node Profile**.
3. Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
4. This brings you to menu 11.1.4. Apply a filter set (our example filter set 3) as shown in Figure 381 on page 555.
5. Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.1.4.

## 38.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyWALL applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyWALL is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

**Figure 378** Protocol and Device Filter Sets



## 38.5 Firewall Versus Filters

Below are some comparisons between the ZyWALL's filtering and firewall functions.

### 38.5.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

#### 38.5.1.1 When To Use Filtering

1. To block/allow LAN packets by their MAC addresses.
2. To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
3. To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. To block/allow IP trace route.

### 38.5.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

#### 38.5.2.1 When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

## 38.6 Applying a Filter

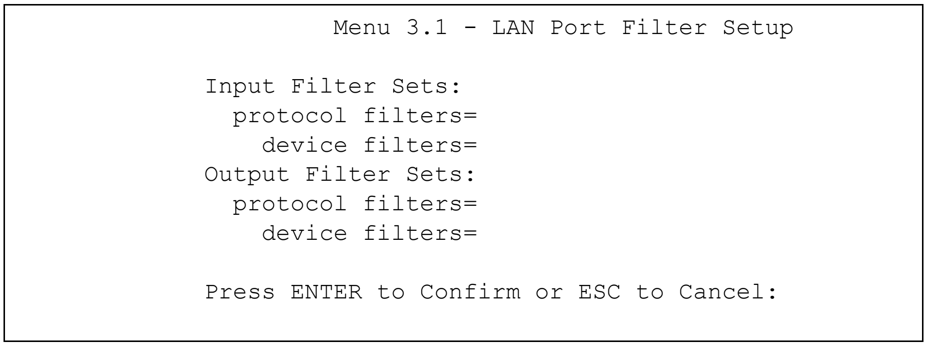
This section shows you where to apply the filter(s) after you design it (them). The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming Telnet, FTP and HTTP connections.

If you do not activate the firewall, it is advisable to apply filters.

## 38.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 379** Filtering LAN Traffic

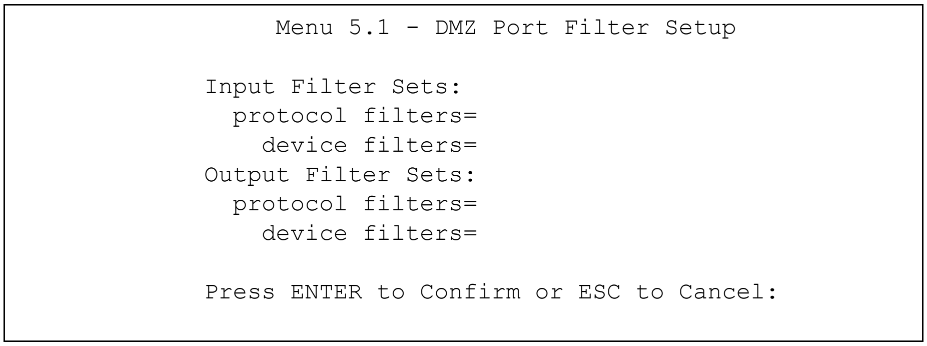


```
                    Menu 3.1 - LAN Port Filter Setup

           Input Filter Sets:
             protocol filters=
               device filters=
           Output Filter Sets:
             protocol filters=
               device filters=

           Press ENTER to Confirm or ESC to Cancel:
```

## 38.6.2 Applying DMZ Filters

DMZ traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 5.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming Telnet, FTP and HTTP connections.

**Figure 380** Filtering DMZ Traffic

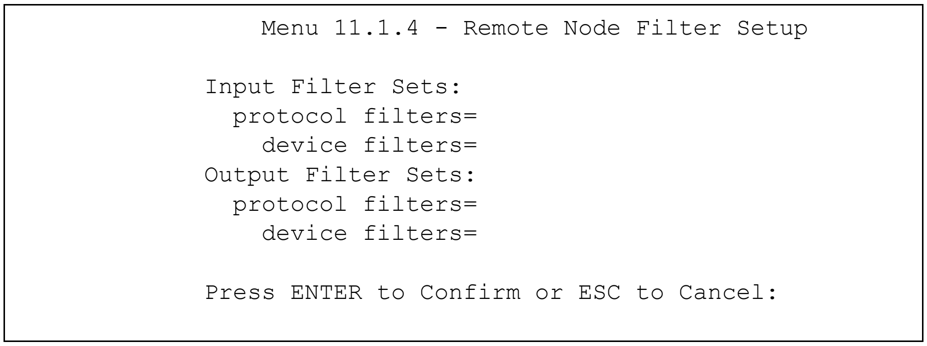


```
                Menu 5.1 - DMZ Port Filter Setup

           Input Filter Sets:
             protocol filters=
               device filters=
           Output Filter Sets:
             protocol filters=
               device filters=

           Press ENTER to Confirm or ESC to Cancel:
```

### 38.6.3 Applying Remote Node Filters

Go to menu 11.1.4 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming Telnet, FTP and HTTP connections.

**Figure 381** Filtering Remote Node Traffic



```
                 Menu 11.1.4 - Remote Node Filter Setup

             Input Filter Sets:
               protocol filters=
                 device filters=
             Output Filter Sets:
               protocol filters=
                 device filters=

             Press ENTER to Confirm or ESC to Cancel:
```

# 39

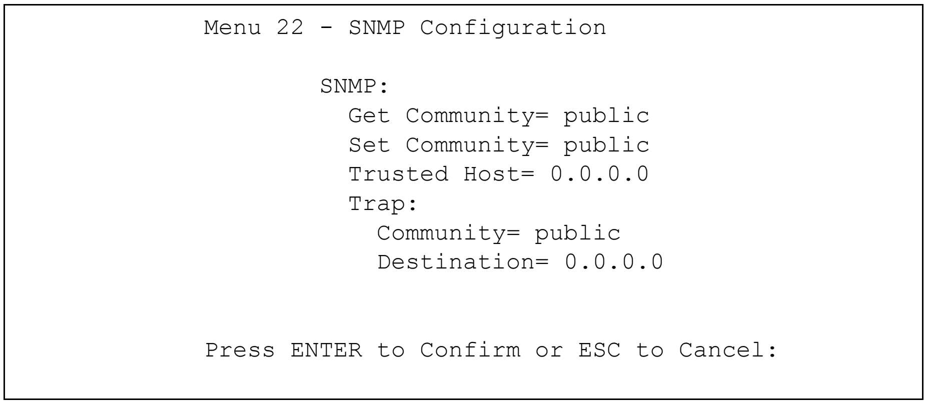
# SNMP Configuration

This chapter explains SNMP configuration menu 22.

## 39.1 SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The “community” for **Get**, **Set** and **Trap** fields is SNMP terminology for password.

**Figure 382** Menu 22: SNMP Configuration



```
              Menu 22 - SNMP Configuration

                      SNMP:
                        Get Community= public
                        Set Community= public
                        Trusted Host= 0.0.0.0
                        Trap:
                          Community= public
                          Destination= 0.0.0.0


              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the SNMP configuration parameters.

**Table 206** SNMP Configuration Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| Get Community | Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station. |
| Set Community | Type the Set community, which is the password for incoming Set requests from the management station. |
| Trusted Host | If you enter a trusted host, your ZyWALL will only respond to SNMP messages from this address. A blank (default) field means your ZyWALL will respond to all SNMP messages it receives, regardless of source. |
| Trap | |
| Community | Type the Trap community, which is the password sent with each trap to the SNMP manager. |

**Table 206** SNMP Configuration Menu Fields (continued)

| FIELD | DESCRIPTION |
|---|---|
| Destination | Type the IP address of the station to send your SNMP traps to. |
| When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

## 39.2 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs:

**Table 207** SNMP Traps

| TRAP # | TRAP NAME | DESCRIPTION |
|---|---|---|
| 0 | coldStart (defined in *RFC-1215*) | A trap is sent after booting (power on). |
| 1 | warmStart (defined in *RFC-1215*) | A trap is sent after booting (software reboot). |
| 4 | authenticationFailure (defined in *RFC-1215*) | A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password). |
| 6 | whyReboot (defined in ZYXEL-MIB) | A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start). |
| 6a | For intentional reboot: | A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.). |
| 6b | For fatal error: | A trap is sent with the message of the fatal code if the system reboots because of fatal errors. |

# 40

# System Information & Diagnosis

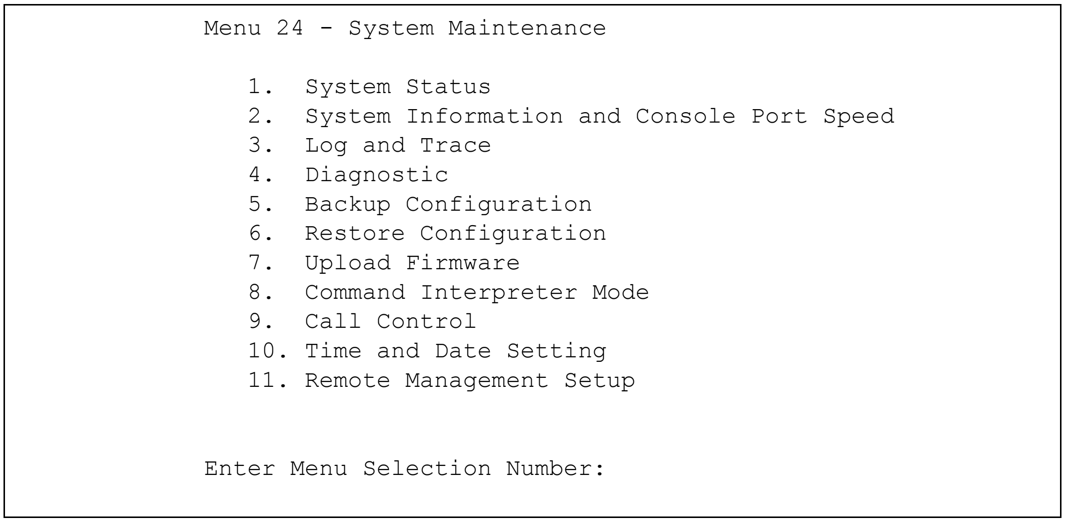
This chapter covers SMT menus 24.1 to 24.4.

## 40.1 Introduction to System Status

This chapter covers the diagnostic tools that help you to maintain your ZyWALL. These tools include updates on system status, port status and log and trace capabilities.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown below.

**Figure 383** Menu 24: System Maintenance



```
              Menu 24 - System Maintenance

                 1.  System Status
                 2.  System Information and Console Port Speed
                 3.  Log and Trace
                 4.  Diagnostic
                 5.  Backup Configuration
                 6.  Restore Configuration
                 7.  Upload Firmware
                 8.  Command Interpreter Mode
                 9.  Call Control
                 10. Time and Date Setting
                 11. Remote Management Setup


              Enter Menu Selection Number:
```

## 40.2 System Status

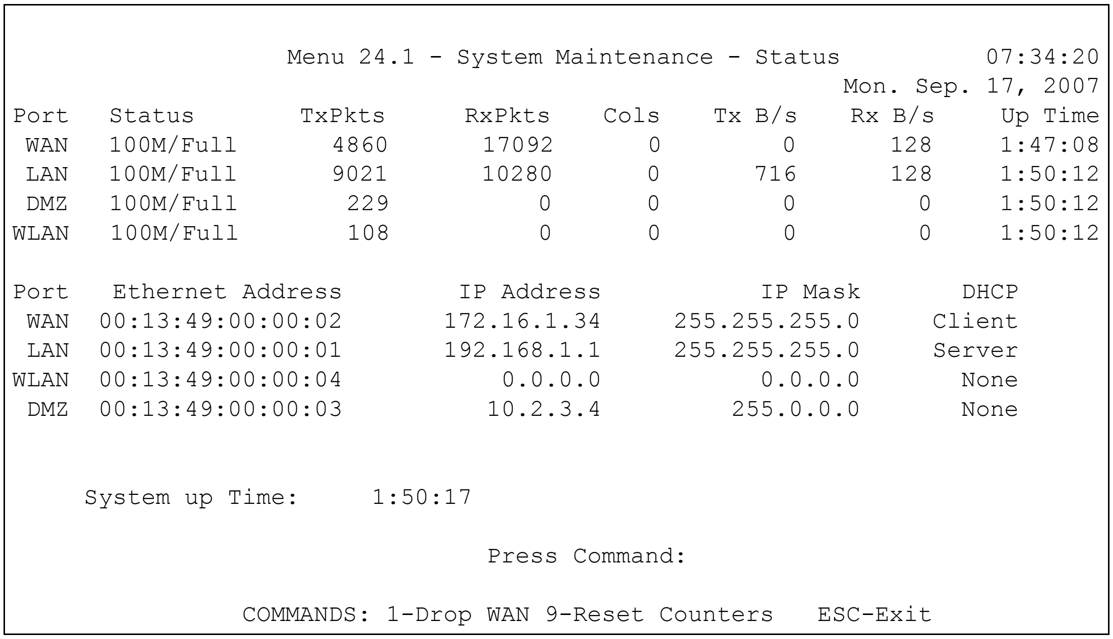
The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your ZyWALL. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

1. Enter number 24 to go to Menu 24 - System Maintenance.
2. In this menu, enter 1 to open System Maintenance - Status.

**3** There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.

**Figure 384** Menu 24.1: System Maintenance: Status



```
                   Menu 24.1 - System Maintenance - Status          07:34:20
                                                         Mon. Sep. 17, 2007
Port   Status        TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
 WAN   100M/Full       4860       17092       0         0       128     1:47:08
 LAN   100M/Full       9021       10280       0       716       128     1:50:12
 DMZ   100M/Full        229           0       0         0         0     1:50:12
WLAN   100M/Full        108           0       0         0         0     1:50:12

Port   Ethernet Address        IP Address          IP Mask       DHCP
 WAN  00:13:49:00:00:02       172.16.1.34     255.255.255.0     Client
 LAN  00:13:49:00:00:01       192.168.1.1     255.255.255.0     Server
WLAN  00:13:49:00:00:04           0.0.0.0           0.0.0.0       None
 DMZ  00:13:49:00:00:03          10.2.3.4         255.0.0.0       None


     System up Time:     1:50:17

                             Press Command:

                COMMANDS: 1-Drop WAN 9-Reset Counters   ESC-Exit
```

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

**Table 208** System Maintenance: Status Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| Port | This field identifies a port (WAN, LAN, DMZ or WLAN) on the ZyWALL. |
| Status | For the LAN, DMZ, and WLAN Interfaces, this displays the port speed and duplex setting.<br>For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation. |
| TxPkts | This is the number of transmitted packets on this port. |
| RxPkts | This is the number of received packets on this port. |
| Cols | This is the number of collisions on this port. |
| Tx B/s | This field shows the transmission speed in Bytes per second on this port. |
| Rx B/s | This field shows the reception speed in Bytes per second on this port. |
| Up Time | This is the total amount of time the line has been up. |
| Ethernet Address | This is the MAC address of the port listed on the left. |
| IP Address | This is the IP address of the port listed on the left. |
| IP Mask | This is the IP mask of the port listed on the left. |
| DHCP | This is the DHCP setting of the port listed on the left. |

**Table 208** System Maintenance: Status Menu Fields (continued)

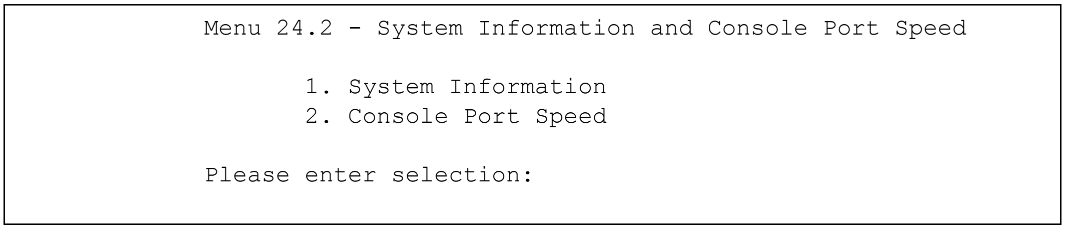
| FIELD | DESCRIPTION |
|---|---|
| System up Time | This is the total time the ZyWALL has been on. |
| You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24. | |

## 40.3 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

1. Enter 24 to go to **Menu 24 - System Maintenance**.
2. Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.
3. From this menu you have two choices as shown in the next figure:

**Figure 385** Menu 24.2: System Information and Console Port Speed

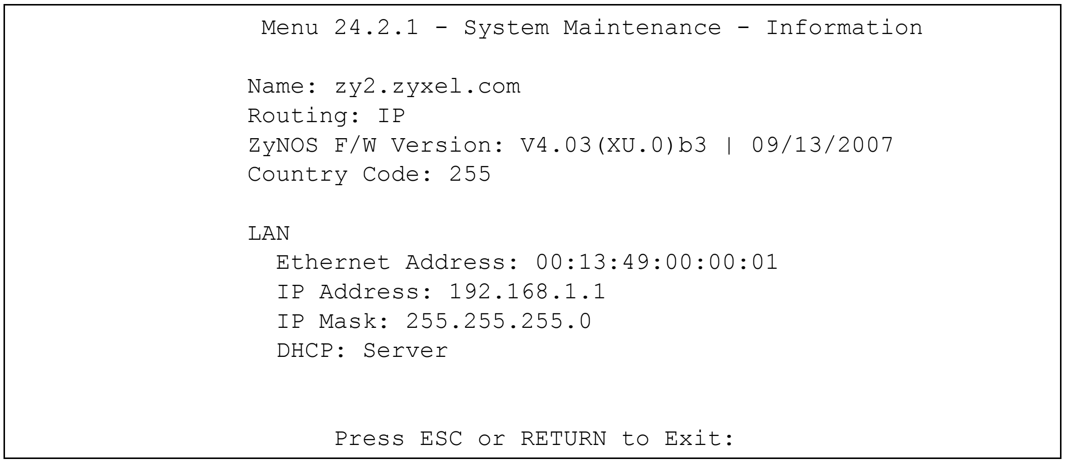


```
             Menu 24.2 - System Information and Console Port Speed

                    1. System Information
                    2. Console Port Speed

             Please enter selection:
```

### 40.3.1 System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

**Figure 386** Menu 24.2.1: System Maintenance: Information



```
                 Menu 24.2.1 - System Maintenance - Information

                Name: zy2.zyxel.com
                Routing: IP
                ZyNOS F/W Version: V4.03(XU.0)b3 | 09/13/2007
                Country Code: 255

                LAN
                  Ethernet Address: 00:13:49:00:00:01
                  IP Address: 192.168.1.1
                  IP Mask: 255.255.255.0
                  DHCP: Server


                      Press ESC or RETURN to Exit:
```

The following table describes the fields in this screen.

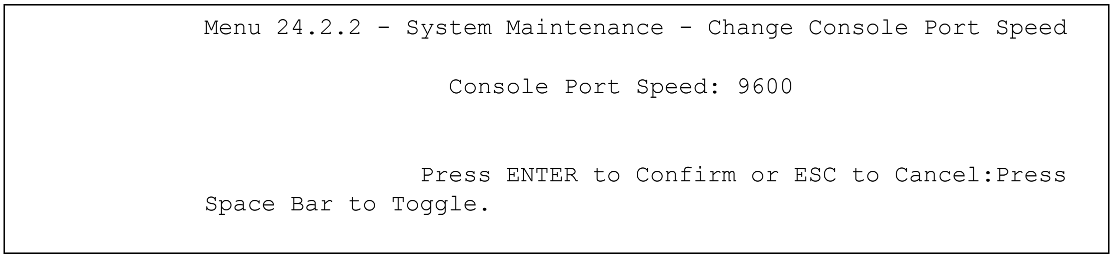
**Table 209** Fields in System Maintenance: Information

| FIELD | DESCRIPTION |
|---|---|
| Name | This is the ZyWALL's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com<br>Name= xxx.baboo.mickey.com |
| Routing | Refers to the routing protocol used. |
| ZyNOS F/W Version | Refers to the version of ZyXEL's Network Operating System software. |
| Country Code | Refers to the country code of the firmware. |
| LAN | |
| Ethernet Address | Refers to the Ethernet MAC (Media Access Control) address of your ZyWALL. |
| IP Address | This is the IP address of the ZyWALL in dotted decimal notation. |
| IP Mask | This shows the IP mask of the ZyWALL. |
| DHCP | This field shows the DHCP setting of the ZyWALL. |
| When finished viewing, press [ESC] or [ENTER] to exit. | |

## 40.3.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your ZyWALL supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown next.

**Figure 387** Menu 24.2.2: System Maintenance: Change Console Port Speed



```
        Menu 24.2.2 - System Maintenance - Change Console Port Speed

                         Console Port Speed: 9600


                      Press ENTER to Confirm or ESC to Cancel:Press
        Space Bar to Toggle.
```

# 40.4 Log and Trace

There are two logging facilities in the ZyWALL. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

## 40.4.1 Viewing Error Log

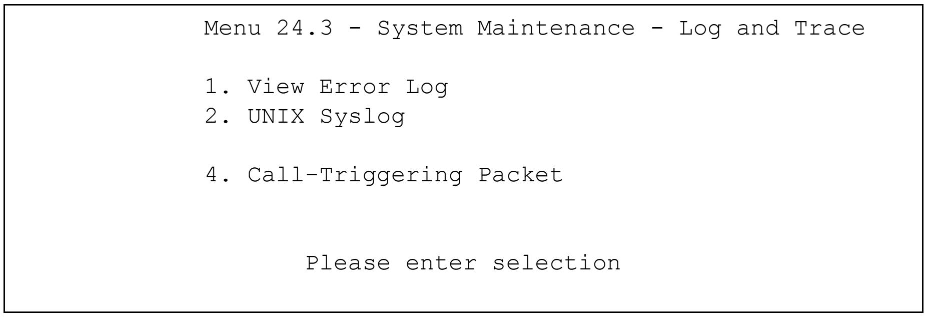
The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

1. Select option 24 from the main menu to open **Menu 24 - System Maintenance**.
2. From menu 24, select option 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.

**3** Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

After the ZyWALL finishes displaying, you will have the option to clear the error log.

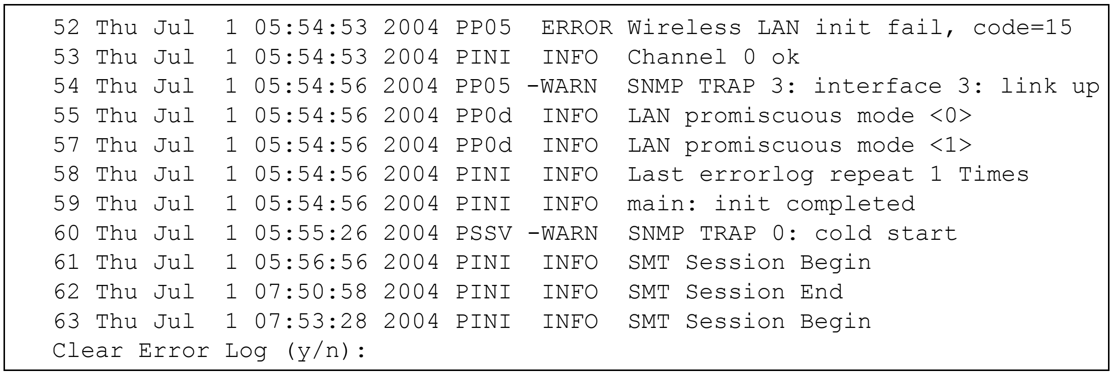
**Figure 388** Menu 24.3: System Maintenance: Log and Trace



```
              Menu 24.3 - System Maintenance - Log and Trace

              1. View Error Log
              2. UNIX Syslog

              4. Call-Triggering Packet


                     Please enter selection
```

Examples of typical error and information messages are presented in the following figure.

**Figure 389** Examples of Error and Information Messages

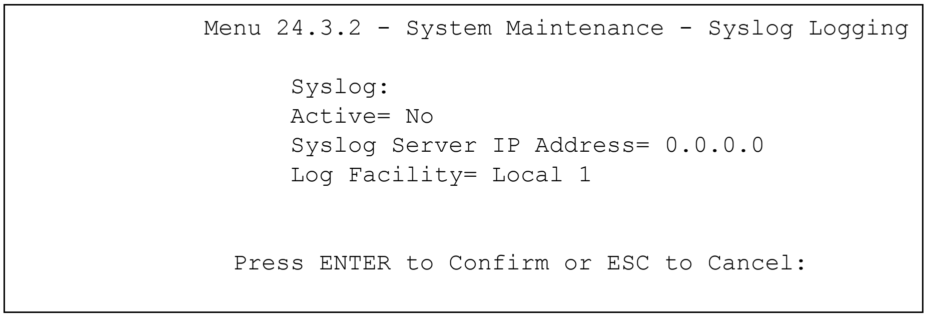


```
   52 Thu Jul  1 05:54:53 2004 PP05  ERROR Wireless LAN init fail, code=15
   53 Thu Jul  1 05:54:53 2004 PINI  INFO  Channel 0 ok
   54 Thu Jul  1 05:54:56 2004 PP05 -WARN  SNMP TRAP 3: interface 3: link up
   55 Thu Jul  1 05:54:56 2004 PP0d  INFO  LAN promiscuous mode <0>
   57 Thu Jul  1 05:54:56 2004 PP0d  INFO  LAN promiscuous mode <1>
   58 Thu Jul  1 05:54:56 2004 PINI  INFO  Last errorlog repeat 1 Times
   59 Thu Jul  1 05:54:56 2004 PINI  INFO  main: init completed
   60 Thu Jul  1 05:55:26 2004 PSSV -WARN  SNMP TRAP 0: cold start
   61 Thu Jul  1 05:56:56 2004 PINI  INFO  SMT Session Begin
   62 Thu Jul  1 07:50:58 2004 PINI  INFO  SMT Session End
   63 Thu Jul  1 07:53:28 2004 PINI  INFO  SMT Session Begin
   Clear Error Log (y/n):
```

## 40.4.2 Syslog Logging

The ZyWALL uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog Logging**, as shown next.

**Figure 390** Menu 24.3.2: System Maintenance: Syslog Logging



```
              Menu 24.3.2 - System Maintenance - Syslog Logging

                    Syslog:
                    Active= No
                    Syslog Server IP Address= 0.0.0.0
                    Log Facility= Local 1


                Press ENTER to Confirm or ESC to Cancel:
```

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

**Table 210** System Maintenance Menu Syslog Parameters

| FIELD | DESCRIPTION |
|---|---|
| Syslog: | |
| Active | Press [SPACE BAR] and then [ENTER] to turn syslog on or off. |
| Syslog Server IP Address | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |
| Log Facility | Press [SPACE BAR] and then [ENTER] to select a location. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel. | |

Your ZyWALL sends five types of syslog messages. Some examples (not all ZyWALL specific) of these syslog messages with their message formats are shown next:

1 CDR

CDR Message Format

```
  SdcmdSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String );
  String = board xx line xx channel xx, call xx, str
  board = the hardware board ID
  line = the WAN ID in a board
  Channel = channel ID within the WAN
  call = the call reference number which starts from 1 and increments by 1 for each new call
  str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
        L02 Tunnel Connected(L2TP)
        C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)
        L02 Call Terminated
        C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2
ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected
64000 40002
Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
```

## 2 Packet triggered

**Packet triggered Message Format**

```
SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
     String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
     Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
     Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002824014000 1f06ac12c0a86614ca849a7b0427001700195b451d1430135004000076000000
```

## 3 Filter log

**Filter log Message Format**

```
SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).
    Src: Source Address
    Dst: Destination Address
    prot: Protocol ("TCP","UDP","ICMP")
spo: Source port
dpo: Destination portMar 03 10:39:43 202.132.155.97 ZyXEL: GEN[ffffffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[ffffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170  dpo=00021]}S04>R01mF
```

**4** PPP log

PPP Log Message Format

```
SdcmdSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing
```

**5** Firewall log

Firewall Log Message Format

```
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol ("TCP","UDP","ICMP", "IGMP", "GRE", "ESP")
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 172.16.1.80     :137  ->172.16.1.80
:137  |UDP|default permit:<2,0>|B
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 192.168.77.88   :520  ->192.168.77.88
:520  |UDP|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.16.1.50     ->172.16.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.16.1.25     ->172.16.1.25
|IGMP<2>|default permit:<2,0>|B
```

## 40.4.3 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

**Figure 391** Call-Triggering Packet Example

```
IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
 Frame Type:

   IP Header:
     IP Version              = 4
     Header Length           = 20
     Type of Service         = 0x00 (0)
     Total Length            = 0x002C (44)
     Identification          = 0x0002 (2)
     Flags                   = 0x00
     Fragment Offset         = 0x00
     Time to Live            = 0xFE (254)
     Protocol                = 0x06 (TCP)
     Header Checksum         = 0xFB20 (64288)
     Source IP               = 0xC0A80101 (192.168.1.1)
     Destination IP          = 0x00000000 (0.0.0.0)

   TCP Header:
     Source Port             = 0x0401 (1025)
     Destination Port        = 0x000D (13)
     Sequence Number         = 0x05B8D000 (95997952)
     Ack Number              = 0x00000000 (0)
     Header Length           = 24
     Flags                   = 0x02 (....S.)
     Window Size             = 0x2000 (8192)
     Checksum                = 0xE06A (57450)
     Urgent Ptr              = 0x0000 (0)
     Options                 =
         0000: 02 04 02 00

   RAW DATA:
     0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E......... ....
     0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00
................
     0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...
```

## 40.5 Diagnostic

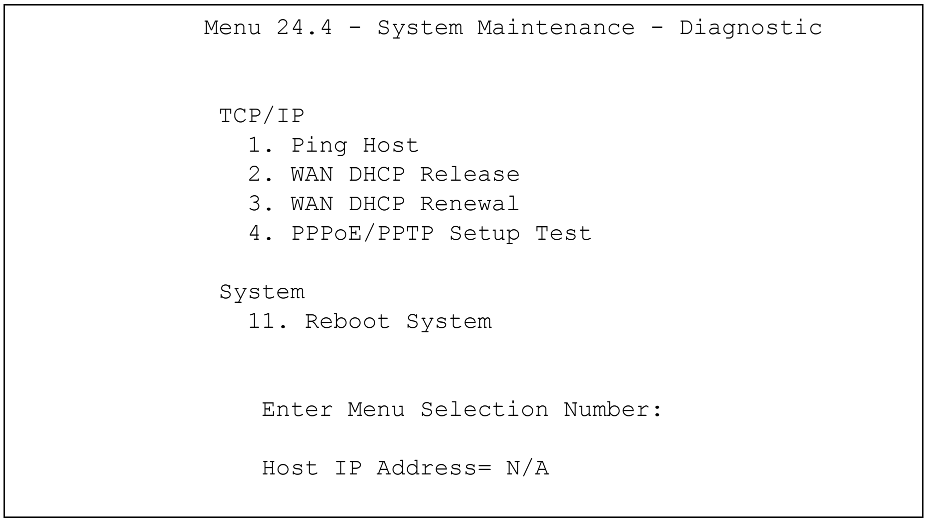
The diagnostic facility allows you to test the different aspects of your ZyWALL to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next. Not all fields are available on all models.

Follow the procedure below to get to **Menu 24.4 - System Maintenance - Diagnostic**.

1 From the main menu, select option 24 to open **Menu 24 - System Maintenance**.

2 From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

**Figure 392** Menu 24.4: System Maintenance: Diagnostic

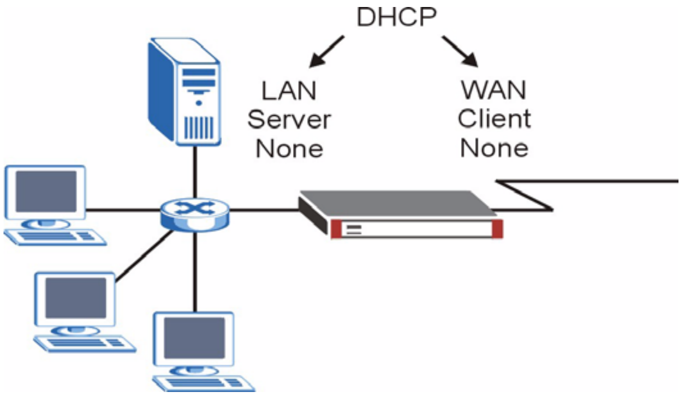


```
                 Menu 24.4 - System Maintenance - Diagnostic


                  TCP/IP
                    1. Ping Host
                    2. WAN DHCP Release
                    3. WAN DHCP Renewal
                    4. PPPoE/PPTP Setup Test

                  System
                    11. Reboot System


                     Enter Menu Selection Number:

                     Host IP Address= N/A
```

## 40.5.1 WAN DHCP

DHCP functionality can be enabled on the LAN, DMZ, WLAN or WAN as shown in Figure 393 on page 568. LAN DHCP has already been discussed. The ZyWALL can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.x.2 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

**Figure 393** WAN & LAN DHCP



The following table describes the diagnostic tests available in menu 24.4 for your ZyWALL and associated connections.

**Table 211** System Maintenance Menu Diagnostic

| FIELD | DESCRIPTION |
|---|---|
| Ping Host | Enter 1 to ping any machine (with an IP address) on your LAN, DMZ, WLAN or WAN. Enter its IP address in the **Host IP Address** field below. |
| WAN DHCP Release | Enter 2 to release your WAN DHCP settings. |

**Table 211** System Maintenance Menu Diagnostic

| FIELD | DESCRIPTION |
|---|---|
| WAN DHCP Renewal | Enter 3 to renew your WAN DHCP settings. |
| PPPoE/PPTP Setup Test | Enter 4 to test the Internet setup. You can also test the Internet setup in **Menu 4 - Internet Access**. Please refer to Chapter 31 on page 497 for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation. |
| Reboot System | Enter 11 to reboot the ZyWALL. |
| Host IP Address | If you entered 1in the **Enter Menu Selection Number** field, then enter the IP address of the computer you want to ping in this field. |
| Enter the number of the selection you would like to perform or press [ESC] to cancel. | |

# 41

# Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

## 41.1 Introduction

Use the instructions in this chapter to change the ZyWALL's configuration file or upgrade its firmware. After you configure your ZyWALL, you can backup the configuration file to a computer. That way if you later misconfigure the ZyWALL, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the ZyWALL to the original default settings. The firmware determines the ZyWALL's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site to use to upgrade your ZyWALL's performance.

## 41.2 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyWALL's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyWALL.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyWALL only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyWALL and the external filename refers to the filename not on the ZyWALL, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 - System Maintenance - Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

**Table 212** Filename Conventions

| FILE TYPE | INTERNAL NAME | EXTERNAL NAME | DESCRIPTION |
|---|---|---|---|
| Configuration File | Rom-0 | This is the configuration filename on the ZyWALL. Uploading the rom-0 file replaces the entire ROM file system, including your ZyWALL configurations, system-related data (including the default password), the error log and the trace log. | *.rom |
| Firmware | Ras | This is the generic name for the ZyNOS firmware on the ZyWALL. | *.bin |

## 41.3 Backup Configuration

The ZyWALL displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 depending on whether you use the console port or Telnet.

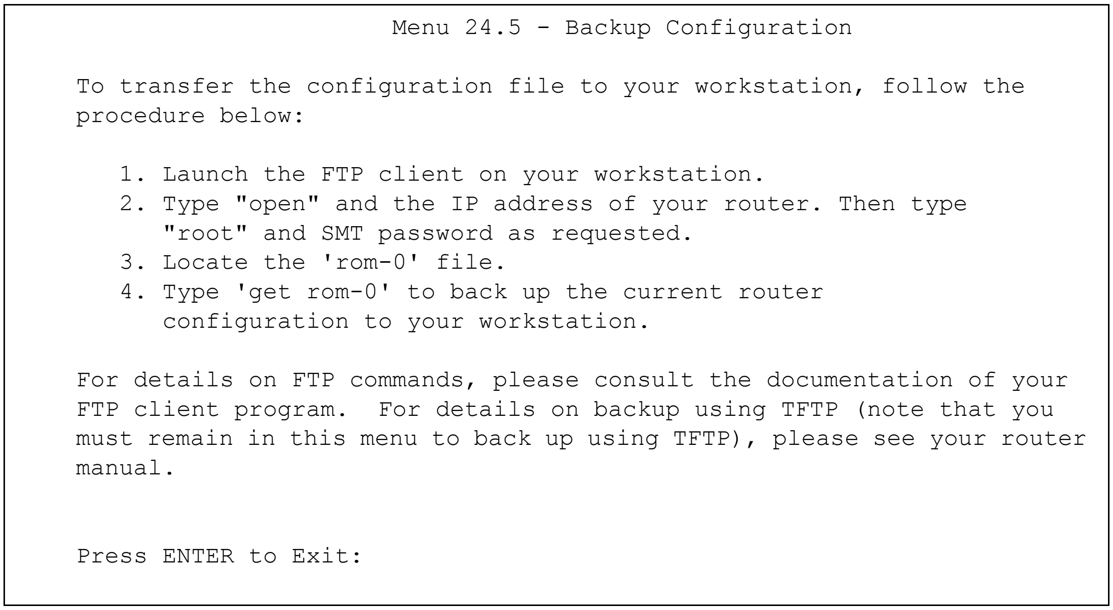
Option 5 from **Menu 24 - System Maintenance** allows you to backup the current ZyWALL configuration to your computer. Backup is highly recommended once your ZyWALL is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the ZyWALL to the computer, while upload means from your computer to the ZyWALL.

### 41.3.1 Backup Configuration

Follow the instructions as shown in the next screen.

**Figure 394** Telnet into Menu 24.5



```
                      Menu 24.5 - Backup Configuration

     To transfer the configuration file to your workstation, follow the
     procedure below:

        1. Launch the FTP client on your workstation.
        2. Type "open" and the IP address of your router. Then type
           "root" and SMT password as requested.
        3. Locate the 'rom-0' file.
        4. Type 'get rom-0' to back up the current router
           configuration to your workstation.

     For details on FTP commands, please consult the documentation of your
     FTP client program.  For details on backup using TFTP (note that you
     must remain in this menu to back up using TFTP), please see your router
     manual.


     Press ENTER to Exit:
```

## 41.3.2 Using the FTP Command from the Command Line

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your ZyWALL.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “get” to transfer files from the ZyWALL to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

### 41.3.3 Example of FTP Commands from the Command Line

**Figure 395** FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

### 41.3.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

**Table 213** General Commands for GUI-based FTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Host Address | Enter the address of the host server. |
| Login Type | Anonymous.<br>This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.<br>Normal.<br>The server requires a unique User ID and Password to login. |
| Transfer Type | Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode |
| Initial Remote Directory | Specify the default remote directory (path). |
| Initial Local Directory | Specify the default local directory (path). |

### 41.3.5 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

1. The firewall is active (turn the firewall off in menu 21.2 or create a firewall rule to allow access from the WAN).
2. You have disabled Telnet service in menu 24.11.
3. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
4. The IP you entered in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyWALL will disconnect the Telnet session immediately.
5. You have an SMT console session running.

## 41.3.6 Backup Configuration Using TFTP

The ZyWALL supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both Telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1. Use Telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the Telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.
5. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).

Note that the Telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyWALL to the computer and “binary” to set binary transfer mode.

## 41.3.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyWALL IP address, “get” transfers the file source on the ZyWALL (rom-0, name of the configuration file on the ZyWALL) to the file destination on the computer and renames it config.rom.

## 41.3.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

**Table 214** General Commands for GUI-based TFTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Host | Enter the IP address of the ZyWALL. 192.168.1.1 is the ZyWALL’s default IP address when shipped. |
| Send/Fetch | Use “Send” to upload the file to the ZyWALL and “Fetch” to back up the file on your computer. |
| Local File | Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer. |

**Table 214** General Commands for GUI-based TFTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Remote File | This is the filename on the ZyWALL. The filename for the firmware is “ras” and for the configuration file, is “rom-0”. |
| Binary | Transfer the file in binary mode. |
| Abort | Stop transfer of the file. |

Refer to Section 41.3.5 on page 574 to read about configurations that disallow TFTP and FTP over WAN.

### 41.3.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.5 and enter “y” at the following screen.

**Figure 396** System Maintenance: Backup Configuration

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

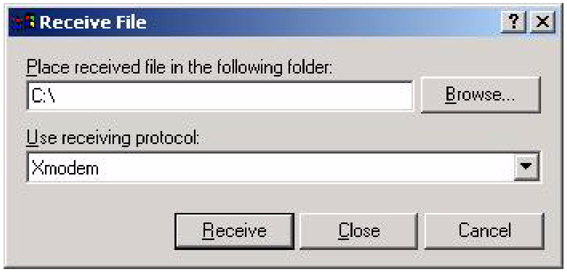
2 The following screen indicates that the Xmodem download has started.

**Figure 397** System Maintenance: Starting Xmodem Download Screen

```
You can enter ctrl-x to terminate operation any
time.
Starting XMODEM download...
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

**Figure 398** Backup Configuration Example



Place received file in the following folder: C:\

Use receiving protocol: Xmodem

Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

**4** After a successful backup you will see the following screen. Press any key to return to the SMT menu.

**Figure 399** Successful Backup Confirmation Screen

```
              ** Backup Configuration completed. OK.
              ### Hit any key to continue.###
```

## 41.4 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

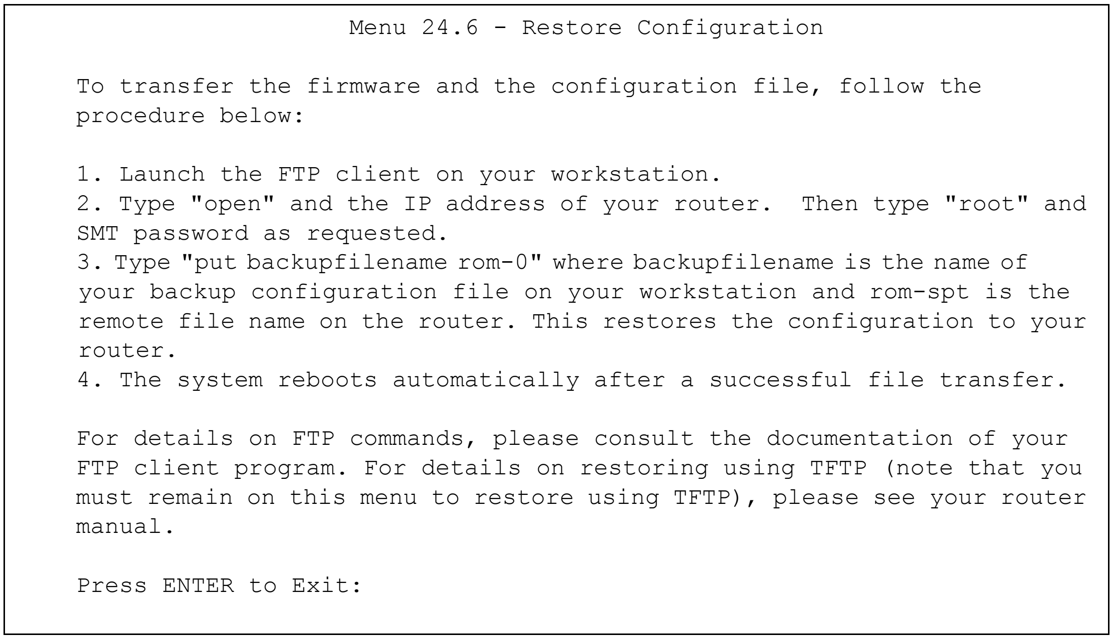
FTP is the preferred method for restoring your current computer configuration to your ZyWALL since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL. When the Restore Configuration process is complete, the ZyWALL will automatically restart.

### 41.4.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

**Figure 400** Telnet into Menu 24.6

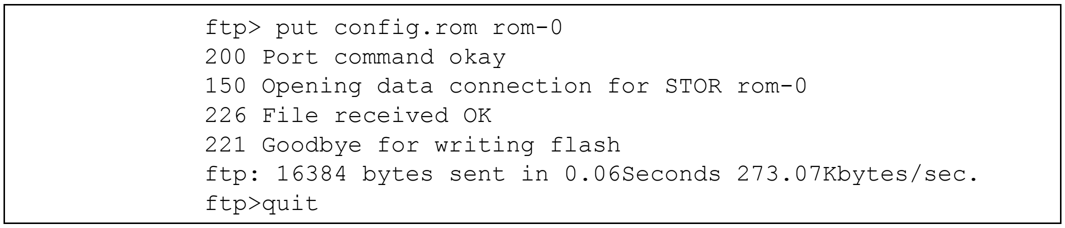


```
                    Menu 24.6 - Restore Configuration

    To transfer the firmware and the configuration file, follow the
    procedure below:

    1. Launch the FTP client on your workstation.
    2. Type "open" and the IP address of your router.  Then type "root" and
    SMT password as requested.
    3. Type "put backupfilename rom-0" where backupfilename is the name of
    your backup configuration file on your workstation and rom-spt is the
    remote file name on the router. This restores the configuration to your
    router.
    4. The system reboots automatically after a successful file transfer.

    For details on FTP commands, please consult the documentation of your
    FTP client program. For details on restoring using TFTP (note that you
    must remain on this menu to restore using TFTP), please see your router
    manual.

    Press ENTER to Exit:
```

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your ZyWALL.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Find the “rom” file (on your computer) that you want to restore to your ZyWALL.
7. Use “put” to transfer files from the ZyWALL to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the ZyWALL. See earlier in this chapter for more information on filename conventions.
8. Enter “quit” to exit the ftp prompt. The ZyWALL will automatically restart after a successful restore process.

### 41.4.2 Restore Using FTP Session Example

**Figure 401** Restore Using FTP Session Example



```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 41.3.5 on page 574 to read about configurations that disallow TFTP and FTP over WAN.

### 41.4.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.6 and enter "y" at the following screen.

**Figure 402** System Maintenance: Restore Configuration

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

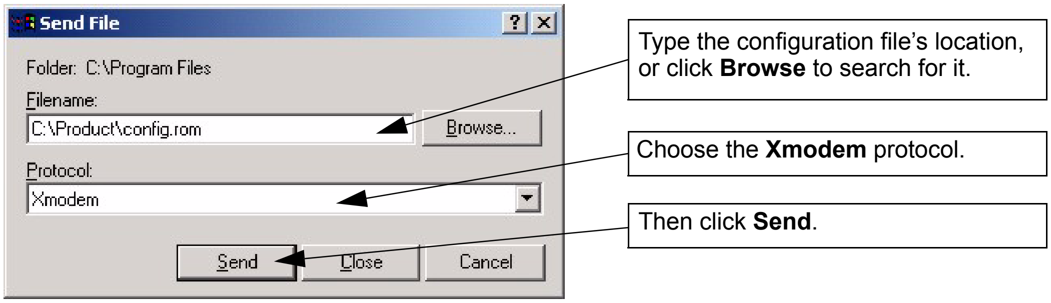
2 The following screen indicates that the Xmodem download has started.

**Figure 403** System Maintenance: Starting Xmodem Download Screen

```
Starting XMODEM download (CRC mode) ...CCCCCCCCC
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

**Figure 404** Restore Configuration Example



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

4 After a successful restoration you will see the following screen. Press any key to restart the ZyWALL and return to the SMT menu.

**Figure 405** Successful Restoration Confirmation Screen

```
Save to ROM
Hit any key to start system reboot.
```

## 41.5 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in Section 41.4 on page 577 or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

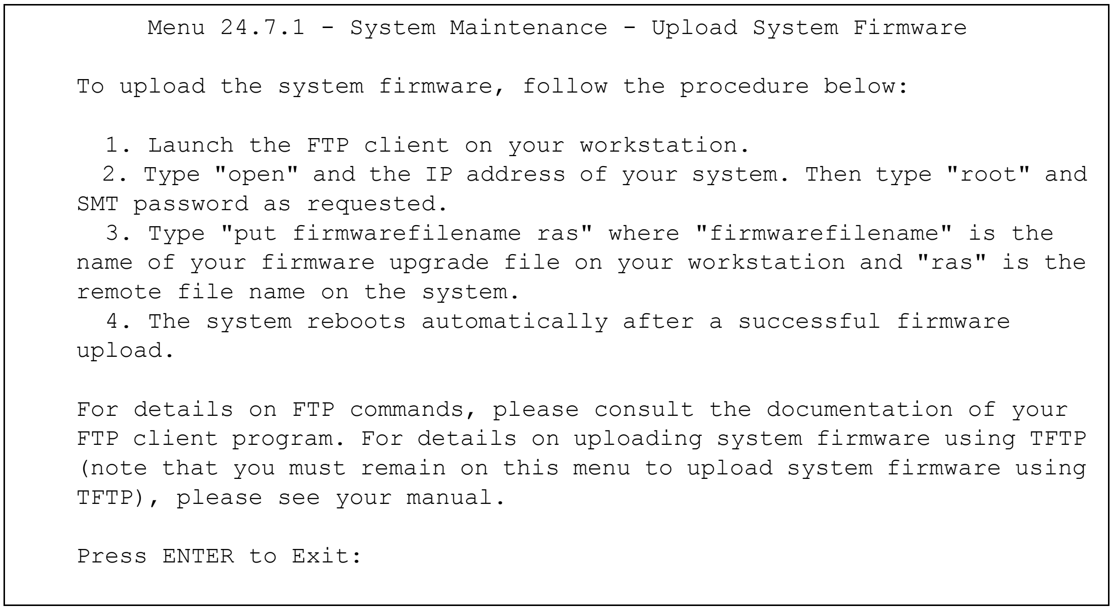
WARNING!
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL.

## 41.5.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you Telnet into the ZyWALL, you will see the following screens for uploading firmware and the configuration file using FTP.

**Figure 406** Telnet Into Menu 24.7.1: Upload System Firmware

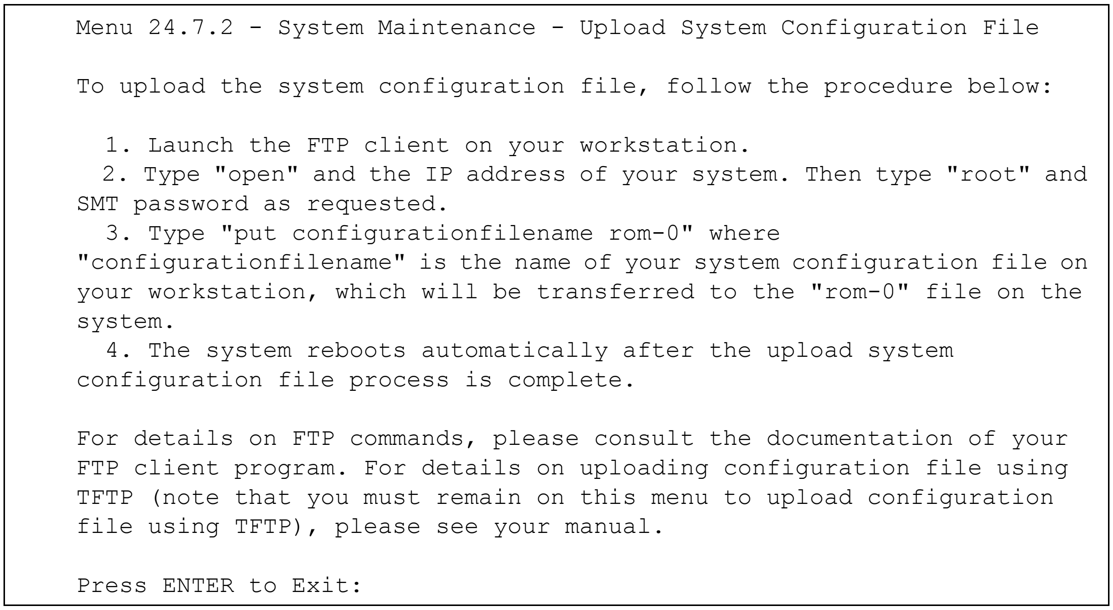


```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

     To upload the system firmware, follow the procedure below:

       1. Launch the FTP client on your workstation.
       2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
       3. Type "put firmwarefilename ras" where "firmwarefilename" is the
     name of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
       4. The system reboots automatically after a successful firmware
     upload.

     For details on FTP commands, please consult the documentation of your
     FTP client program. For details on uploading system firmware using TFTP
     (note that you must remain on this menu to upload system firmware using
     TFTP), please see your manual.

     Press ENTER to Exit:
```

## 41.5.2 Configuration File Upload

You see the following screen when you Telnet into menu 24.7.2.

**Figure 407** Telnet Into Menu 24.7.2: System Maintenance



```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
SMT password as requested.
  3. Type "put configurationfilename rom-0" where
"configurationfilename" is the name of your system configuration file on
your workstation, which will be transferred to the "rom-0" file on the
system.
  4. The system reboots automatically after the upload system
configuration file process is complete.

For details on FTP commands, please consult the documentation of your
FTP client program. For details on uploading configuration file using
TFTP (note that you must remain on this menu to upload configuration
file using TFTP), please see your manual.

Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

### 41.5.3 FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your ZyWALL.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the ZyWALL, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyWALL and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyWALL and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

### 41.5.4 FTP Session Example of Firmware File Upload

**Figure 408** FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to Section 41.3.5 on page 574 to read about configurations that disallow TFTP and FTP over WAN.

### 41.5.5 TFTP File Upload

The ZyWALL also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both Telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use Telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the Telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.
5. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the firmware is “ras”.

Note that the Telnet connection must be active and the ZyWALL in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyWALL to the computer, “put” the other way around, and “binary” to set binary transfer mode.

### 41.5.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyWALL’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyWALL).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

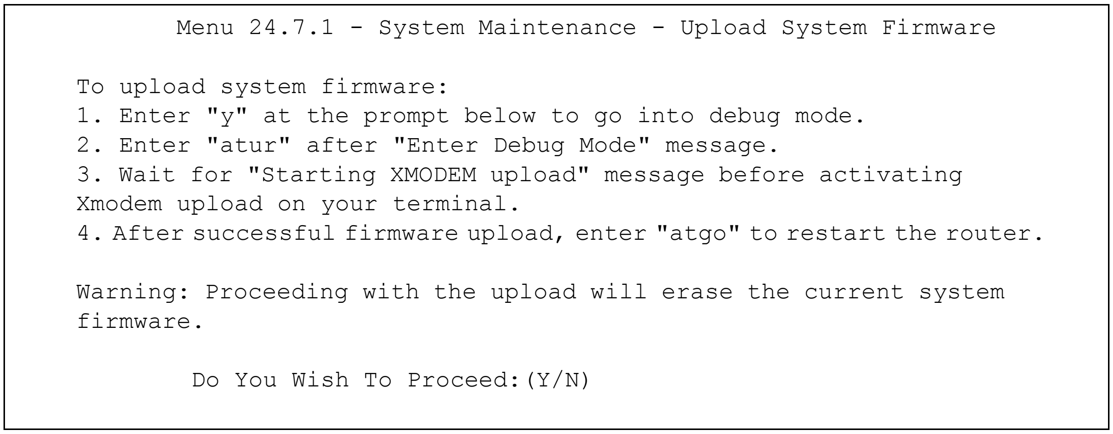
### 41.5.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyWALL. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyWALL via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

### 41.5.8 Uploading Firmware File Via Console Port

1 Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 - System Maintenance - Upload System Firmware**, and then follow the instructions as shown in the following screen.

**Figure 409** Menu 24.7.1 As Seen Using the Console Port



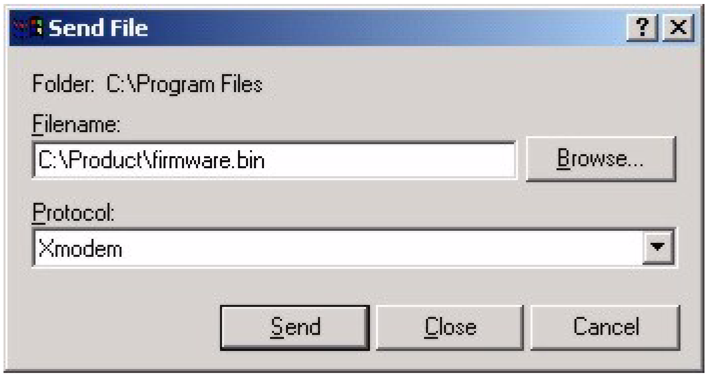
```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

  To upload system firmware:
  1. Enter "y" at the prompt below to go into debug mode.
  2. Enter "atur" after "Enter Debug Mode" message.
  3. Wait for "Starting XMODEM upload" message before activating
  Xmodem upload on your terminal.
  4. After successful firmware upload, enter "atgo" to restart the router.

  Warning: Proceeding with the upload will erase the current system
  firmware.

          Do You Wish To Proceed:(Y/N)
```

2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

### 41.5.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

**Figure 410** Example Xmodem Upload



Folder: C:\Program Files

Filename: C:\Product\firmware.bin

Protocol: Xmodem

After the firmware upload process has completed, the ZyWALL will automatically restart.

### 41.5.10 Uploading Configuration File Via Console Port

1 Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 - System Maintenance - Upload System Configuration File**. Follow the instructions as shown in the next screen.

**Figure 411** Menu 24.7.2 As Seen Using the Console Port

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart
   the system.

Warning:
1. Proceeding with the upload will erase the current
configuration file.
2. The system's console port speed (Menu 24.2.2) may change when it is
restarted; please adjust your terminal's speed accordingly. The password
may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
port speed will be reset to 9600 bps and the password to "1234".

         Do You Wish To Proceed:(Y/N)
```

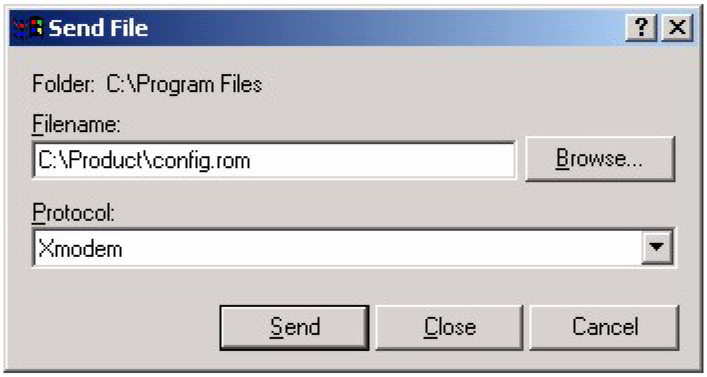
2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter “atgo” to restart the ZyWALL.

### 41.5.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

**Figure 412** Example Xmodem Upload



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

After the configuration upload process has completed, restart the ZyWALL by entering "atgo".

# 42

# System Maintenance Menus 8 to 10

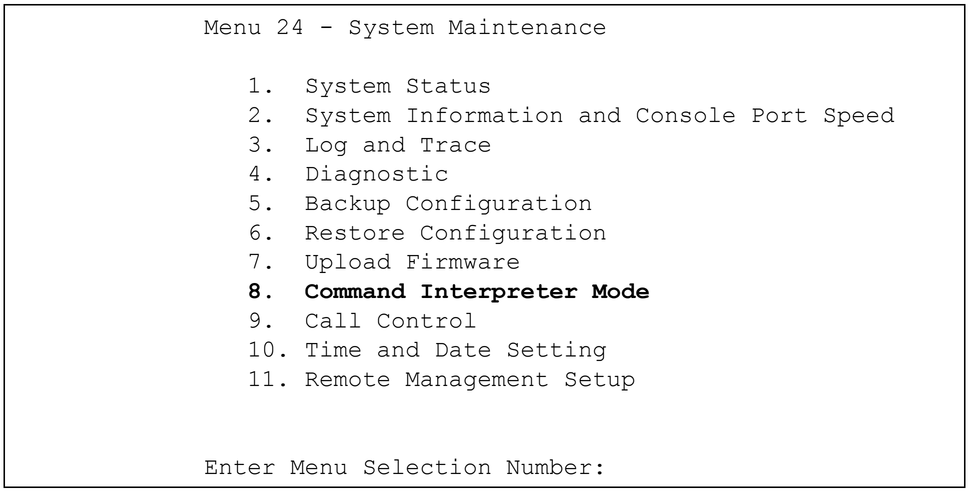
This chapter leads you through SMT menus 24.8 to 24.10.

## 42.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or zyxel.com for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

**Figure 413** Command Mode in Menu 24



```
              Menu 24 - System Maintenance

                 1.  System Status
                 2.  System Information and Console Port Speed
                 3.  Log and Trace
                 4.  Diagnostic
                 5.  Backup Configuration
                 6.  Restore Configuration
                 7.  Upload Firmware
                 8.  Command Interpreter Mode
                 9.  Call Control
                 10. Time and Date Setting
                 11. Remote Management Setup


              Enter Menu Selection Number:
```

## 42.1.1 Command Syntax

The command keywords are in `courier new` font.

Enter the command keywords exactly as shown, do not abbreviate.

The required fields in a command are enclosed in angle brackets <>.

The optional fields in a command are enclosed in square brackets `[]`.

The `|` symbol means "or".

For example,

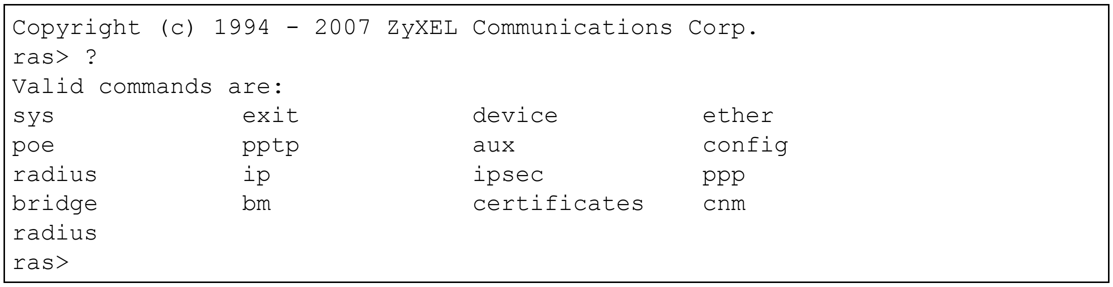
```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

## 42.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

**Figure 414** Valid Commands



```
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
poe             pptp            aux             config
radius          ip              ipsec           ppp
bridge          bm              certificates    cnm
radius
ras>
```

The following table describes some commands in this screen.

**Table 215** Valid Commands

| COMMAND | DESCRIPTION |
|---|---|
| sys | The system commands display device information and configure device settings. |
| exit | This command returns you to the SMT main menu. |
| device | The device commands deal with the dial backup connection. |
| ether | These commands display Ethernet information and configure Ethernet settings. |
| aux | These commands display dial backup information and control dial backup connections. |
| ip | These commands display IP information and configure IP settings. |
| ipsec | These commands display IPSec information and configure IPSec settings. |
| bridge | These commands display bridge information. |
| bm | These commands configure bandwidth management settings and display bandwidth management information. |
| certificates | These commands display certificate information and configure certificate settings. |

## 42.2 Call Control Support

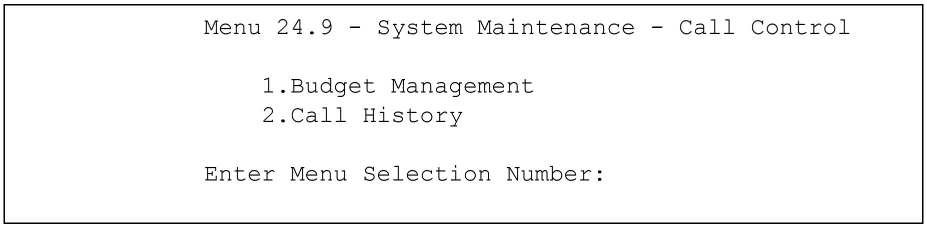
The ZyWALL provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyWALL within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

**Figure 415** Call Control

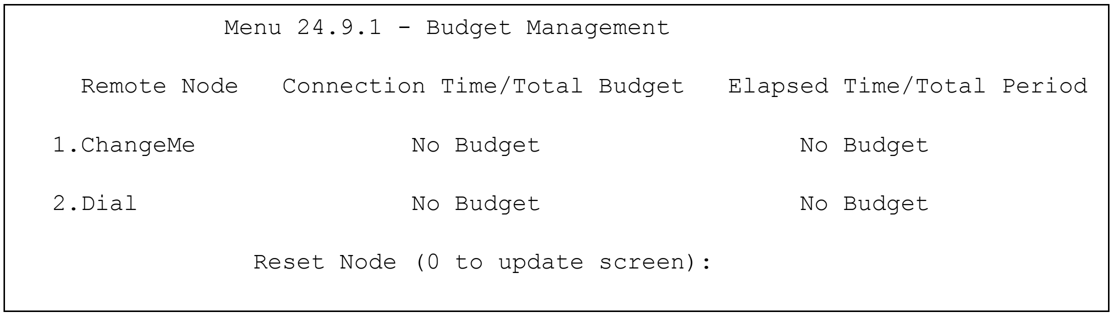


```
              Menu 24.9 - System Maintenance - Call Control

                  1.Budget Management
                  2.Call History

              Enter Menu Selection Number:
```

### 42.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

**Figure 416** Budget Management



```
               Menu 24.9.1 - Budget Management

     Remote Node   Connection Time/Total Budget   Elapsed Time/Total Period

   1.ChangeMe               No Budget                  No Budget

   2.Dial                   No Budget                  No Budget

                 Reset Node (0 to update screen):
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

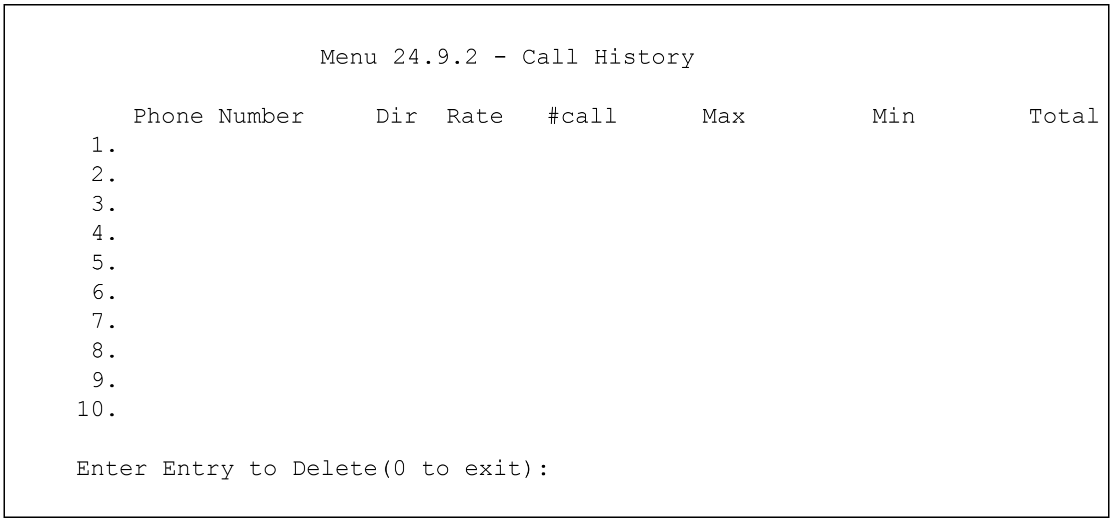
**Table 216** Budget Management

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Remote Node | Enter the index number of the remote node you want to reset (just one in this case) | 1 |
| Connection Time/ Total Budget | This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1). | 5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed. |
| Elapsed Time/Total Period | The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period. | 0.5/1 means that 30 minutes out of the 1-hour time period has lapsed. |
| Enter “0” to update the screen or press [ESC] to return to the previous screen. | | |

## 42.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

**Figure 417** Call History



```
                    Menu 24.9.2 - Call History

        Phone Number     Dir  Rate   #call      Max         Min        Total
     1.
     2.
     3.
     4.
     5.
     6.
     7.
     8.
     9.
    10.

    Enter Entry to Delete(0 to exit):
```

The following table describes the fields in this screen.

**Table 217** Call History

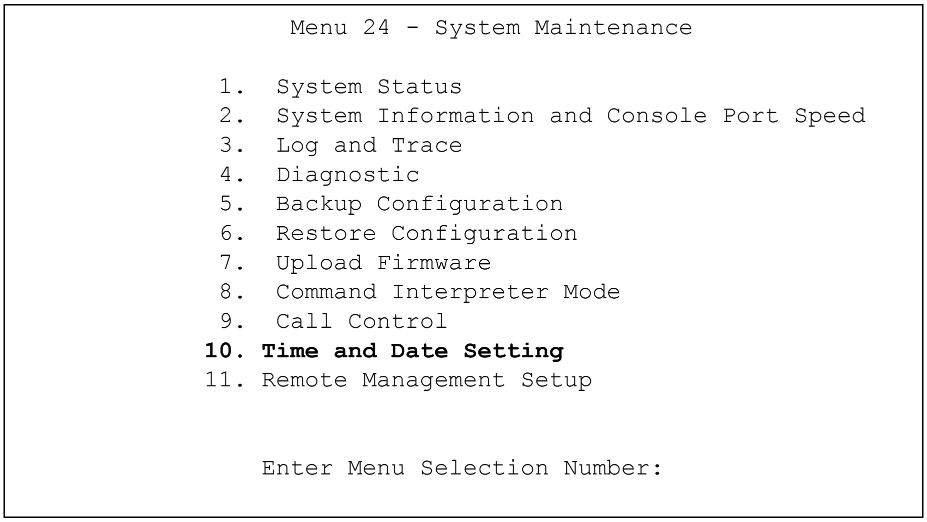
| FIELD | DESCRIPTION |
|---|---|
| Phone Number | The PPPoE service names are shown here. |
| Dir | This shows whether the call was incoming or outgoing. |
| Rate | This is the transfer rate of the call. |
| #call | This is the number of calls made to or received from that telephone number. |
| Max | This is the length of time of the longest telephone call. |
| Min | This is the length of time of the shortest telephone call. |
| Total | This is the total length of time of all the telephone calls to/from that telephone number. |
| You may enter an entry number to delete it or ‘”0” to exit. | |

## 42.3 Time and Date Setting

The ZyWALL’s Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL. Menu 24.10 allows you to update the time and date settings of your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

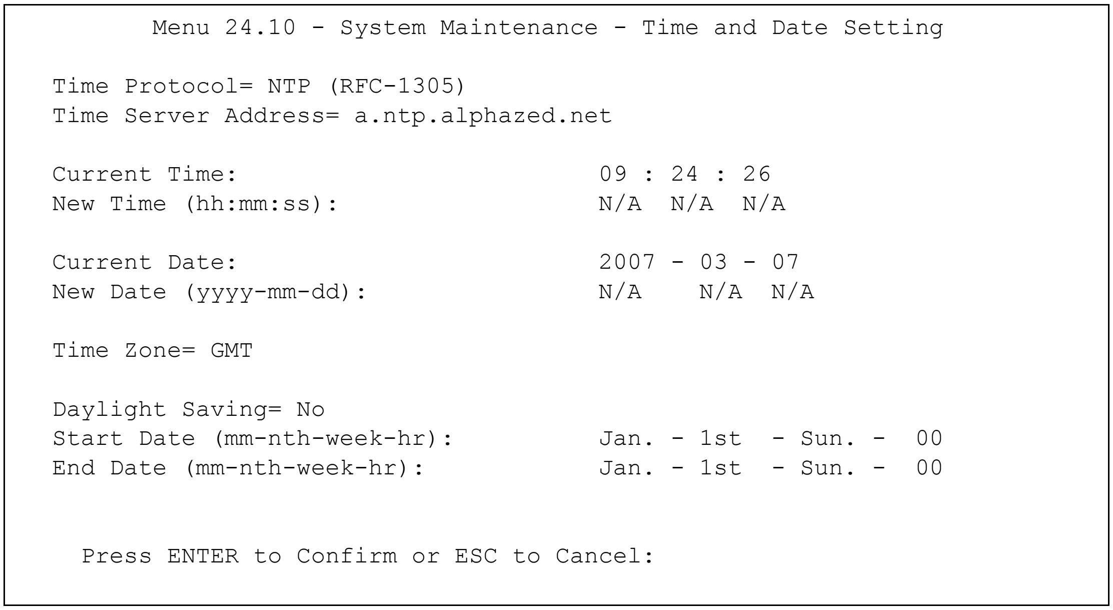
**Figure 418** Menu 24: System Maintenance



```
                    Menu 24 - System Maintenance

               1.  System Status
               2.  System Information and Console Port Speed
               3.  Log and Trace
               4.  Diagnostic
               5.  Backup Configuration
               6.  Restore Configuration
               7.  Upload Firmware
               8.  Command Interpreter Mode
               9.  Call Control
              10. Time and Date Setting
              11. Remote Management Setup


                  Enter Menu Selection Number:
```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your ZyWALL as shown in the following screen.

**Figure 419** Menu 24.10 System Maintenance: Time and Date Setting



```
         Menu 24.10 - System Maintenance - Time and Date Setting

  Time Protocol= NTP (RFC-1305)
  Time Server Address= a.ntp.alphazed.net

  Current Time:                        09 : 24 : 26
  New Time (hh:mm:ss):                 N/A  N/A  N/A

  Current Date:                        2007 - 03 - 07
  New Date (yyyy-mm-dd):               N/A    N/A  N/A

  Time Zone= GMT

  Daylight Saving= No
  Start Date (mm-nth-week-hr):         Jan. - 1st  - Sun. -  00
  End Date (mm-nth-week-hr):           Jan. - 1st  - Sun. -  00


    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 218** Menu 24.10 System Maintenance: Time and Date Setting

| FIELD | DESCRIPTION |
|---|---|
| Time Protocol | Enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>The default, **NTP (RFC-1305)**, is similar to **Time (RFC-868)**.<br>Select **Manual** to enter the new time and new date manually. |
| Time Server Address | Enter the IP address or domain name of your timeserver. Check with your ISP/ network administrator if you are unsure of this information. |
| Current Time | This field displays an updated time only when you reenter this menu. |
| New Time | Enter the new time in hour, minute and second format. This field is available when you select **Manual** in the **Time Protocol** field. |
| Current Date | This field displays an updated date only when you reenter this menu. |
| New Date | Enter the new date in year, month and day format. This field is available when you select **Manual** in the **Time Protocol** field. |
| Time Zone | Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Daylight Saving | Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose **Yes**. |

**Table 218** Menu 24.10 System Maintenance: Time and Date Setting

| FIELD | DESCRIPTION |
|---|---|
| Start Date (mm-nth-week-hr) | Configure the day and time when Daylight Saving Time starts if you selected **Yes** in the **Daylight Saving** field. The **hr** field uses the 24 hour format. Here are a couple of examples:<br>Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Apr.**, **1st**, **Sun.** and type 02 in the **hr** field.<br>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Mar.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Date (mm-nth-week-hr) | Configure the day and time when Daylight Saving Time ends if you selected **Yes** in the **Daylight Saving** field. The **hr** field uses the 24 hour format. Here are a couple of examples:<br>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Oct.**, **Last**, **Sun.** and type 02 in the **hr** field.<br>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Oct.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel. | |

# 43

# Remote Management

This chapter covers remote management found in SMT menu 24.11.

## 43.1 Remote Management

Remote management allows you to determine which services/protocols can access which ZyWALL interface (if any) from which computers.

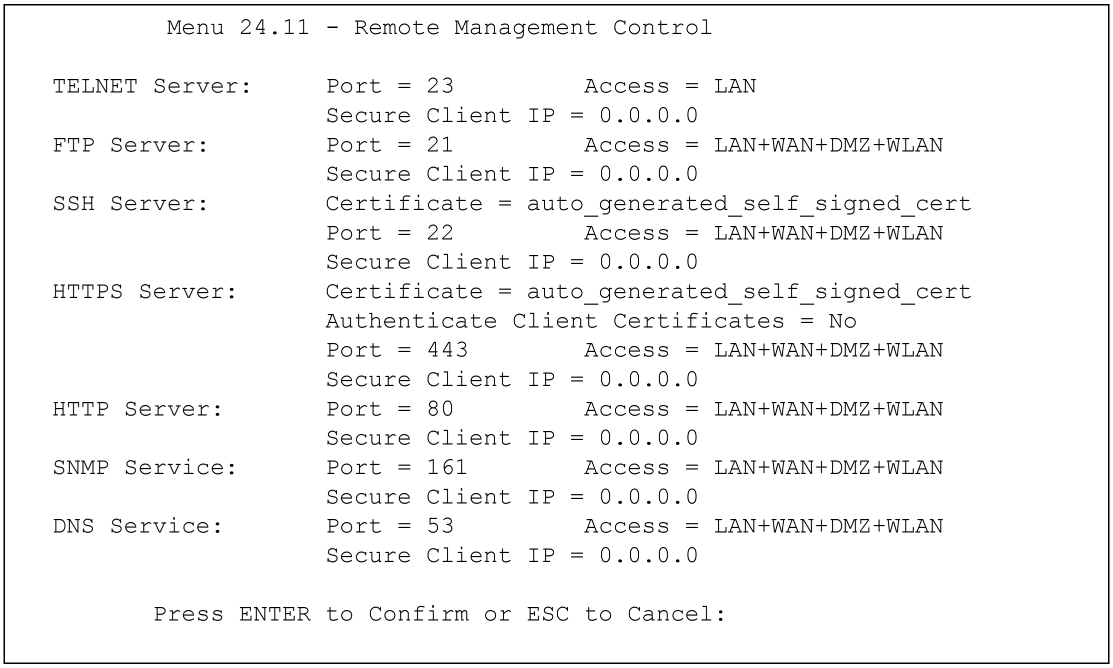
When you configure remote management to allow management from any network except the LAN, you still need to configure a firewall rule to allow access. See Chapter 11 on page 191 for details on configuring firewall rules.

You can also disable a service on the ZyWALL by not allowing access for the service/protocol through any of the ZyWALL interfaces.

To disable remote management of a service, select **Disable** in the corresponding **Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 - Remote Management Control**.

**Figure 420**   Menu 24.11 – Remote Management Control



```
          Menu 24.11 - Remote Management Control

  TELNET Server:      Port = 23         Access = LAN
                      Secure Client IP = 0.0.0.0
  FTP Server:         Port = 21         Access = LAN+WAN+DMZ+WLAN
                      Secure Client IP = 0.0.0.0
  SSH Server:         Certificate = auto_generated_self_signed_cert
                      Port = 22         Access = LAN+WAN+DMZ+WLAN
                      Secure Client IP = 0.0.0.0
  HTTPS Server:       Certificate = auto_generated_self_signed_cert
                      Authenticate Client Certificates = No
                      Port = 443        Access = LAN+WAN+DMZ+WLAN
                      Secure Client IP = 0.0.0.0
  HTTP Server:        Port = 80         Access = LAN+WAN+DMZ+WLAN
                      Secure Client IP = 0.0.0.0
  SNMP Service:       Port = 161        Access = LAN+WAN+DMZ+WLAN
                      Secure Client IP = 0.0.0.0
  DNS Service:        Port = 53         Access = LAN+WAN+DMZ+WLAN
                      Secure Client IP = 0.0.0.0

         Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 219**   Menu 24.11 – Remote Management Control

| FIELD | DESCRIPTION |
|---|---|
| Telnet Server<br>FTP Server<br>SSH Server<br>HTTPS Server<br>HTTP Server<br>SNMP Service<br>DNS Service | Each of these read-only labels denotes a service that you may use to remotely manage the ZyWALL. |
| Port | This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the ZyWALL. |
| Access | Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN**, **WAN**, **LAN+WAN**, **DMZ**, **LAN+DMZ**, **WAN+DMZ**, **LAN+WAN+DMZ**, **WLAN**, **LAN+WLAN**, **WAN+WLAN**, **LAN+WAN+WLAN**, **DMZ+WLAN**, **LAN+DMZ+WLAN**, **WAN+DMZ+WLAN**, **LAN+WAN+DMZ+WLAN** or **Disable**. |
| Secure Client IP | The default 0.0.0.0 allows any client to use this service to remotely manage the ZyWALL. Enter an IP address to restrict access to a client with a matching IP address. |
| Certificate | Press [SPACE BAR] and then [ENTER] to select the certificate that the ZyWALL will use to identify itself. The ZyWALL is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL). |

**Table 219** Menu 24.11 – Remote Management Control (continued)

| FIELD | DESCRIPTION |
|---|---|
| Authenticate Client Certificates | Select **Yes** by pressing [SPACE BAR], then [ENTER] to require the SSL client to authenticate itself to the ZyWALL by sending the ZyWALL a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyWALL (see Appendix E on page 657 for details). |
| Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel. | |

### 43.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
6. There is a firewall rule that blocks it.

# 44

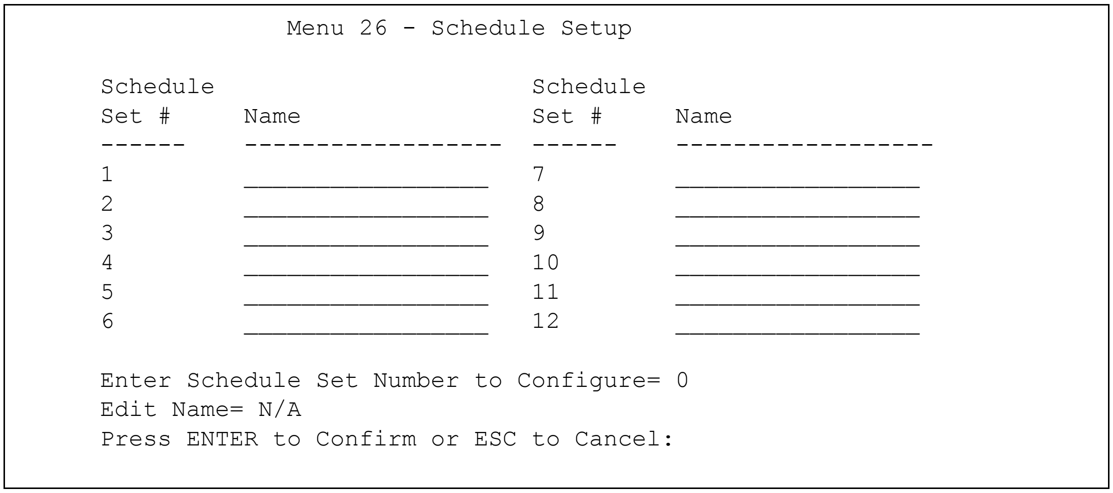
# Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

## 44.1 Introduction to Call Scheduling

The call scheduling feature allows the ZyWALL to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next.

**Figure 421** Schedule Setup



```
                     Menu 26 - Schedule Setup

      Schedule                      Schedule
      Set #     Name                Set #     Name
      ------    ------------------  ------    ------------------
      1         _________________   7         _________________
      2         _________________   8         _________________
      3         _________________   9         _________________
      4         _________________   10        _________________
      5         _________________   11        _________________
      6         _________________   12        _________________

      Enter Schedule Set Number to Configure= 0
      Edit Name= N/A
      Press ENTER to Confirm or ESC to Cancel:
```

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node, then set 1 will take precedence over set 2, 3 and 4 as the ZyWALL, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] or [DEL] in the Edit Name field.

To set up a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

**Figure 422** Schedule Set Setup

```
              Menu 26.1 - Schedule Set Setup

              Active= Yes
              How Often= Once
              Start Date(yyyy-mm-dd) = N/A
              Once:
                Date(yyyy-mm-dd)= 2000 - 01 - 01
              Weekdays:
                Sunday= N/A
                Monday= N/A
                Tuesday= N/A
                Wednesday= N/A
                Thursday= N/A
                Friday= N/A
                Saturday= N/A
              Start Time (hh:mm)= 00 : 00
              Duration (hh:mm)= 00 : 00
              Action= Forced On

              Press ENTER to Confirm or ESC to Cancel:
              Press Space Bar to Toggle
```

If a connection has been already established, your ZyWALL will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

**Table 220** Schedule Set Setup

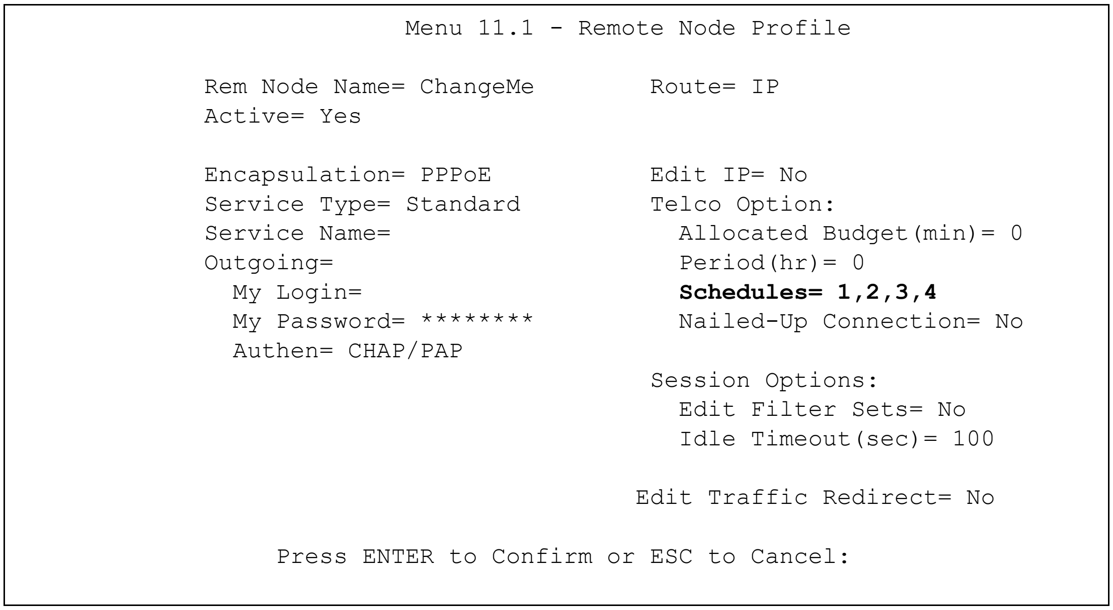
| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set. |
| How Often | Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses. |
| Start Date | Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5. |
| Once: | |
| Date | If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format. |
| Weekdays: | |

**Table 220** Schedule Set Setup (continued)

| FIELD | DESCRIPTION |
|---|---|
| Day | If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER]. |
| Start Time | Enter the start time when you wish the schedule set to take effect in hour-minute format. |
| Duration | The duration determines how long the ZyWALL is to apply the action configured in the **Action** field. Enter the maximum length of time in hour-minute format. |
| Action | **Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field.<br>**Forced Down** means that the connection is blocked whether or not there is a demand call on the line.<br>**Enable Dial-On-Demand** means that this schedule permits a demand call on the line.<br>**Disable Dial-On-Demand** means that this schedule prevents a demand call on the line. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the Main Menu and then enter the target remote node index. Press [SPACE BAR] and then [ENTER] to select **PPPoE** in the **Encapsulation** field to make the schedule sets field available as shown next.

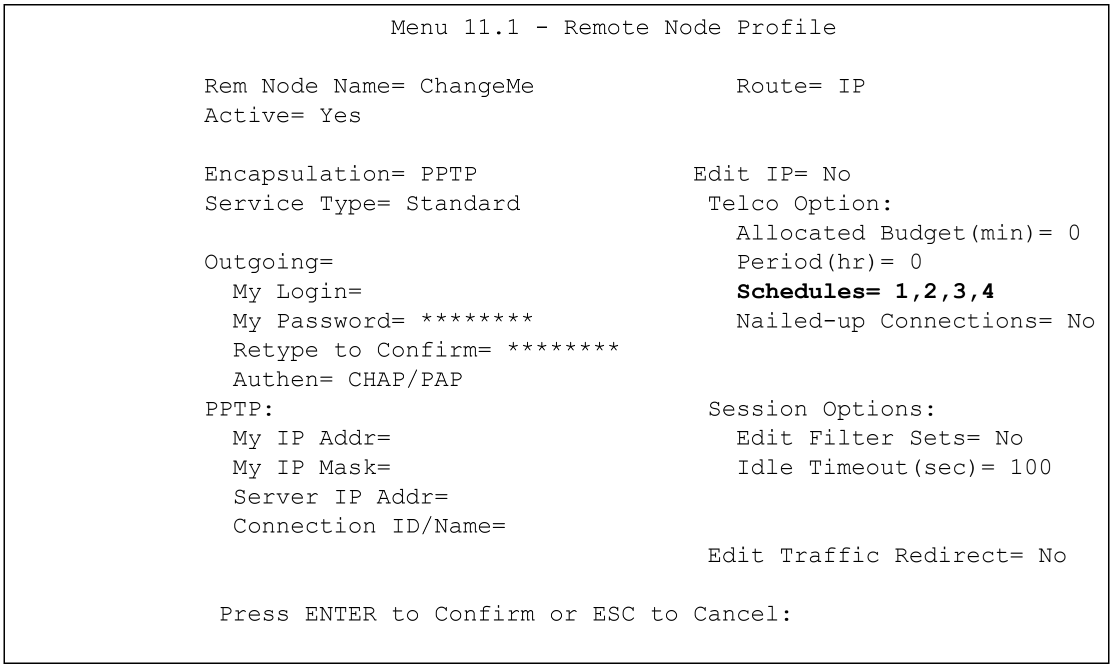
**Figure 423** Applying Schedule Set(s) to a Remote Node (PPPoE)



```
                     Menu 11.1 - Remote Node Profile

              Rem Node Name= ChangeMe        Route= IP
              Active= Yes

              Encapsulation= PPPoE           Edit IP= No
              Service Type= Standard         Telco Option:
              Service Name=                    Allocated Budget(min)= 0
              Outgoing=                        Period(hr)= 0
                My Login=                      Schedules= 1,2,3,4
                My Password= ********          Nailed-Up Connection= No
                Authen= CHAP/PAP
                                             Session Options:
                                               Edit Filter Sets= No
                                               Idle Timeout(sec)= 100

                                            Edit Traffic Redirect= No

                   Press ENTER to Confirm or ESC to Cancel:
```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

**Figure 424** Applying Schedule Set(s) to a Remote Node (PPTP)



```
                           Menu 11.1 - Remote Node Profile

              Rem Node Name= ChangeMe              Route= IP
              Active= Yes

              Encapsulation= PPTP               Edit IP= No
              Service Type= Standard             Telco Option:
                                                   Allocated Budget(min)= 0
              Outgoing=                            Period(hr)= 0
                My Login=                          Schedules= 1,2,3,4
                My Password= ********              Nailed-up Connections= No
                Retype to Confirm= ********
                Authen= CHAP/PAP
              PPTP:                              Session Options:
                My IP Addr=                        Edit Filter Sets= No
                My IP Mask=                        Idle Timeout(sec)= 100
                Server IP Addr=
                Connection ID/Name=
                                                 Edit Traffic Redirect= No

               Press ENTER to Confirm or ESC to Cancel:
```

# PART VII

# Troubleshooting and Specifications

Troubleshooting (605)
Product Specifications (613)

# 45

# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyWALL Access and Login
- Internet Access
- Wireless Router/AP Troubleshooting
- UPnP

## 45.1 Power, Hardware Connections, and LEDs

### The ZyWALL does not turn on. None of the LEDs turn on when you turn on the ZyWALL.

7. Make sure you are using the power adaptor or cord included with the ZyWALL.
8. Make sure the power adaptor or cord is connected to the ZyWALL and plugged in to an appropriate power source. Make sure the power source is turned on.
9. Disconnect and re-connect the power adaptor or cord to the ZyWALL.
10. If the problem continues, contact the vendor.

### One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 49.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor to the ZyWALL.
5. If the problem continues, contact the vendor.

## 45.2 ZyWALL Access and Login

### I forgot the IP address for the ZyWALL.

1. The default IP address is **192.168.1.1**.
2. Use the console port to log in to the ZyWALL.
3. If you changed the IP address and have forgotten it, you might get the IP address of the ZyWALL by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyWALL (it depends on the network), so enter this IP address in your Internet browser.
4. If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 53.

### I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 53.

### I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default LAN IP address is 192.168.1.1. If you changed the LAN IP address (Section 6.7 on page 136), enter the new one as the URL.
   - If you changed the LAN IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyWALL.
   - Use the ZyWALL's WAN IP address when configuring from the WAN.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide .
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 637.
4. Make sure your computer is in the same subnet as the ZyWALL for LAN access. (If you know that there are routers between your computer and the ZyWALL, skip this step.)
   - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix A on page 621. Your ZyWALL is a DHCP server by default.
5. Reset the device to its factory defaults, and try to access the ZyWALL with the default IP address. See Section 2.3 on page 53.

6. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- You may also need to clear your Internet browser's cache.

  In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Options** screen.

  In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it.
- If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).

  In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.
- Try to access the ZyWALL using another service, such as Telnet. If you can access the ZyWALL, check the remote management settings, firewall rules, and SMT filters to find out why the ZyWALL does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN** port.

## I can see the **Login** screen, but I cannot log in to the ZyWALL.

1. Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
2. You cannot log in to the web configurator while someone is using the SMT, Telnet, or the console port to access the ZyWALL. Log out of the ZyWALL in the other session, or ask the person who is logged in to log out.
3. Disconnect and re-connect the power adaptor or cord to the ZyWALL.
4. If this does not work, you have to reset the device to its factory defaults. See Section 2.3 on page 53.

## I cannot access the SMT. / I cannot Telnet to the ZyWALL.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

## I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

### I cannot use the console port to access the ZyWALL.

1. Check to see if the ZyWALL is connected to your computer's console port.
2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:
    - VT100 terminal emulation.
    - 9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
    - No parity, 8 data bits, 1 stop bit, data flow set to none.

### I cannot ping any computer on the LAN.

1. Check the 10M/100M LAN LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your ZyWALL and hub or the station.
2. Verify that the IP address and the subnet mask of the ZyWALL and the computers are on the same subnet.

### I cannot access servers on the DMZ from the LAN.

1. Check your Ethernet cable type and connections. Refer to the Quick Start Guide for DMZ connection instructions.
2. Make sure the Ethernet adapters on the LAN computer and the DMZ server are installed and functioning properly.
3. Verify that the IP address of the DMZ port and the LAN port are on separate subnets.
4. Make sure that NAT is configured for your DMZ servers.

## 45.3 Internet Access

### I cannot get a WAN IP address from the ISP.

1. The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.

The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Refer to the WAN setup chapter (web configurator or SMT).

2. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
3. If the problem continues, contact your ISP.

## I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 49.
2. Make sure you entered your ISP account information correctly in the wizard, WAN screen or SMT menu. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5. If the problem continues, contact your ISP.

## I cannot access the Internet anymore. I had access to the Internet (with the ZyWALL), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 49.
2. Check the schedule rules. Refer to Chapter 44 on page 599 (SMT).
3. If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to the Chapter 8 on page 151 (web configurator) or Chapter 31 on page 497 (SMT).
4. Reboot the ZyWALL.
5. If the problem continues, contact your ISP.

## The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 49. If the ZyWALL is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the ZyWALL closer to the AP if possible, and look around to see if there are any devices that might be

interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3. Reboot the ZyWALL.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.

## 45.4 Wireless Router/AP Troubleshooting

I cannot access the ZyWALL or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the ZyWALL
2. Make sure the wireless adapter on the wireless station is working properly.
3. Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the ZyWALL.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the ZyWALL.
5. Check that both the ZyWALL and your wireless station are using the same wireless and wireless security settings.
6. Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the ZyWALL.
7. Make sure you allow the ZyWALL to be remotely accessed through the WLAN interface. Check your remote management settings.

## 45.5 UPnP

When using UPnP and the ZyWALL reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1. Disconnect the Ethernet cable from the ZyWALL’s LAN port or from your computer.
2. Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

## I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1. Wait more than three minutes.
2. Restart the applications.

# 46

# Product Specifications

his chapter gives details about your ZyWALL's hardware and firmware features.

## 46.1 General ZyWALL Specifications

The following tables summarize the ZyWALL's hardware and firmware features.

**Table 221** Hardware Specifications

| | |
|---|---|
| Dimensions (W x D x H) | 181(W) x 128(D) x 36(H) mm |
| Weight | 304g |
| Power Specification | 12 V DC 1 A |
| Ethernet Ports | Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode.<br>Auto-crossover: Use either crossover or straight-through Ethernet cables. |
| Reset Button | Restores factory default settings |
| Console | RJ-45 port for RS-232 null modem connection |
| Dial Backup | RJ-45 port for RS-232 connection |
| Operation Temperature | 0º C ~ 50º C |
| Storage Temperature | -30º C ~ 60º C |
| Operation Humidity | 20% ~ 95% RH (non-condensing) |
| Storage Humidity | 20% ~ 95% RH (non-condensing) |
| Distance between the centers of the holes (for wall mounting) on the ZyWALL's back. | 125 mm |
| Recommended type of screws for wall-mounting | M4 Tap Screw, see Figure 427 on page 618. |
| Certifications | EMC: FCC Class B, CE-EMC Class B, C-Tick Class B, VCCI Class B<br>Safety: CSA International, CE EN60950-1 |

**Table 222** Firmware Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Default IP Address | 192.168.1.1 |
| Default Subnet Mask | 255.255.255.0 (24 bits) |
| Default Password | 1234 |
| DHCP Pool | 192.168.1.33 to 192.168.1.160 |

**Table 222** Firmware Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Device Management | Use the web configurator to easily configure the rich range of features on the ZyWALL. |
| Firmware Upgrade | Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyWALL.<br>Note: Only upload firmware for your specific model! |
| Configuration Backup & Restoration | Make a copy of the ZyWALL's configuration. You can put it back on the ZyWALL later if you decide to revert back to an earlier configuration. |
| Network Address Translation (NAT) | Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network. |
| Port Forwarding | If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet. |
| DHCP (Dynamic Host Configuration Protocol) | Use this feature to have the ZyWALL assign IP addresses, an IP default gateway and DNS servers to computers on your network. |
| Dynamic DNS Support | With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider. |
| IP Multicast | IP multicast is used to send traffic to a specific group of computers. The ZyWALL supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236). |
| IP Alias | IP alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the ZyWALL itself as the gateway for each subnet. |
| Time and Date | Get the current time and date from an external server when you turn on your ZyWALL. You can also set the time manually. These dates and times are then used in logs. |
| Logging and Tracing | Use packet tracing and logs for troubleshooting. You can send logs from the ZyWALL to an external syslog server. |
| PPPoE | PPPoE mimics a dial-up Internet access connection. |
| PPTP Encapsulation | Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The ZyWALL supports one PPTP connection at a time. |
| Universal Plug and Play (UPnP) | A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network. |
| RoadRunner Support | The ZyWALL supports Time Warner's RoadRunner Service in addition to standard cable modem services. |
| Firewall | You can configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example. |
| Content Filter | The ZyWALL blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering.<br>You can also subscribe to category-based content filtering that allows your ZyWALL to check web sites against an external database. |

**Table 222** Firmware Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Bandwidth Management | You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers. |
| Remote Management | This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyWALL. |

**Table 223** Feature and Performance Specifications

| FEATURE | SPECIFICATION |
|---|---|
| Local User Database Entries | 32 |
| Static DHCP Table Entries | 32 |
| Static Routes | 12 |
| Port Forwarding Rules | 20 |
| Concurrent Sessions (NAT sessions) | 3000 |
| Address Mapping Rules | 10 |
| Configurable IPSec VPN Network Policies (including network policies in the recycle bin) | 10 |
| Simultaneous IPSec VPN Connections | 5 |
| Bandwidth Management Classes | 10 |
| Bandwidth Management Class Levels | 1 |
| DNS Address Record Entries | 30 |
| DNS Name Server Record Entries | 16 |
| Firewall Throughput | 24Mbps |
| VPN 3DES/AES Throughput | 24Mbps |
| User Licenses | Unlimited |

## 46.2 Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The ZyWALL is DCE when you connect a computer to the console port. The ZyWALL is DTE when you connect a modem to the dial backup port.[1]

The console cable and dial backup cable each have an RJ-45 connector and a DB-9 connector. The pin layout for the DB-9 connector end of the cables is as follows.

---

[1] Pins 2,3 and 5 are used.

**Figure 425** Console/Dial Backup Cable DB-9 End Pin Layout

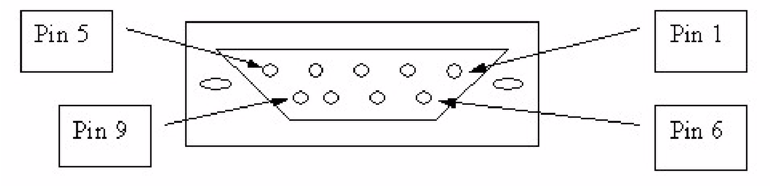


**Table 224** Console Cable Pin Assignments

| PIN DEFINITION | RJ-45 END | DB-9M (MALE) END |
|---|---|---|
| DSR | 1 | 6 |
| DTR | 2 | 4 |
| TX | 3 | 3 |
| RTS | 4 | 7 |
| GND | 5 | 5 |
| RX | 6 | 2 |
| CTS | 7 | 8 |
| DCD | 8 | 1 |
|  | N/A | 9 |

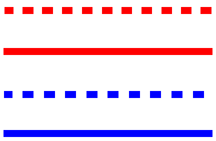
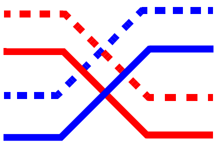
**Table 225** Dial Backup Cable Pin Assignments

| PIN DEFINITION | RJ-45 END | DB-9M (MALE) END |
|---|---|---|
| DTR | 1 | 4 |
| DSR | 2 | 6 |
| RX | 3 | 2 |
| CTS | 4 | 8 |
| GND | 5 | 5 |
| TX | 6 | 3 |
| RTS | 7 | 7 |
| DCD | 8 | 1 |
|  | N/A | 9 |

**Table 226** Ethernet Cable Pin Assignments

| WAN / LAN ETHERNET CABLE PIN LAYOUT | | | |
|---|---|---|---|
| **Straight-through** | | **Crossover** | |
| (Switch) | (Adapter) | (Switch) | (Switch) |

**Table 226** Ethernet Cable Pin Assignments

| WAN / LAN ETHERNET CABLE PIN LAYOUT | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | IRD + |  | 1 | OTD + | 1 | IRD + |  | 1 | IRD + |
| 2 | IRD - | | 2 | OTD - | 2 | IRD - | | 2 | IRD - |
| 3 | OTD + | | 3 | IRD + | 3 | OTD + | | 3 | OTD + |
| 6 | OTD - | | 6 | IRD - | 6 | OTD - | | 6 | OTD - |

## 46.3 Wall-mounting Instructions

Complete the following steps to hang your ZyWALL on a wall.

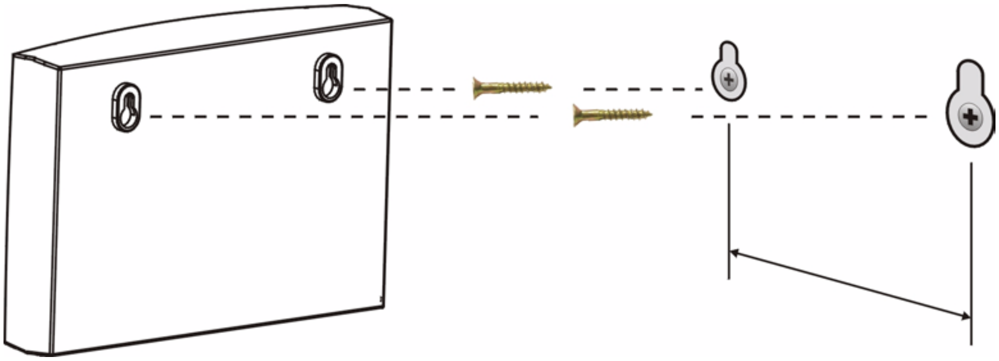
See Table 221 on page 613 for the size of screws to use and how far apart to place them.

1. Select a position free of obstructions on a sturdy wall.
2. Drill two holes for the screws.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

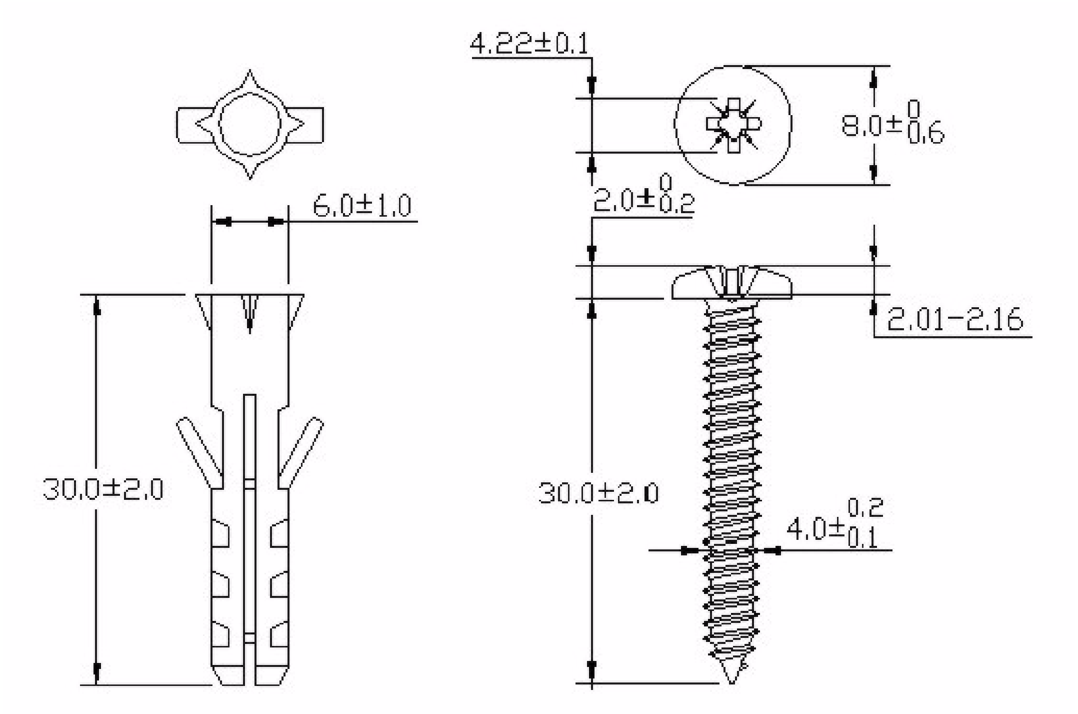
3. Do not insert the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
4. Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyWALL with the connection cables.
5. Align the holes on the back of the ZyWALL with the screws on the wall. Hang the ZyWALL on the screws.

**Figure 426** Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

**Figure 427** Masonry Plug and M4 Tap Screw


4.22±0.1
8.0± 0 0.6
2.0± 0 0.2
6.0±1.0
2.01−2.16
30.0±2.0
30.0±2.0
4.0± 0.2 0.1

# PART VIII

# Appendices and Index

The appendices provide general information. Some details may not apply to your ZyWALL.

Setting up Your Computer’s IP Address (621)
Pop-up Windows, JavaScripts and Java Permissions (637)
IP Addresses and Subnetting (645)
Common Services (653)
Importing Certificates (657)
Legal Information (669)
Customer Support (673)
Index (679)

# A

# Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

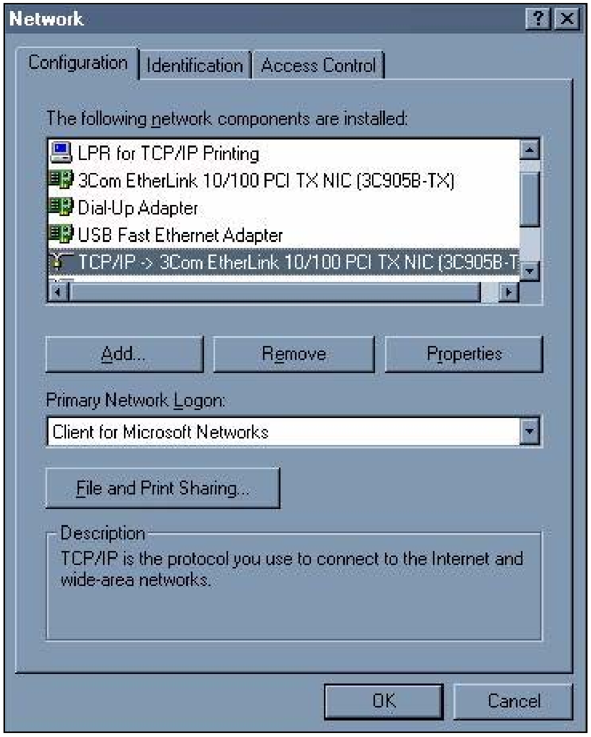
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyWALL's LAN port.

## Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 428** WIndows 95/98/Me: Network: Configuration



The following network components are installed:

- LPR for TCP/IP Printing
- 3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
- Dial-Up Adapter
- USB Fast Ethernet Adapter
- TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.
2 Select **Adapter** and then click **Add**.
3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.
2 Select **Protocol** and then click **Add**.
3 Select **Microsoft** from the list of **manufacturers**.
4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.
2 Select **Client** and then click **Add**.
3 Select **Microsoft** from the list of manufacturers.
4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5 Restart your computer so the changes you made take effect.

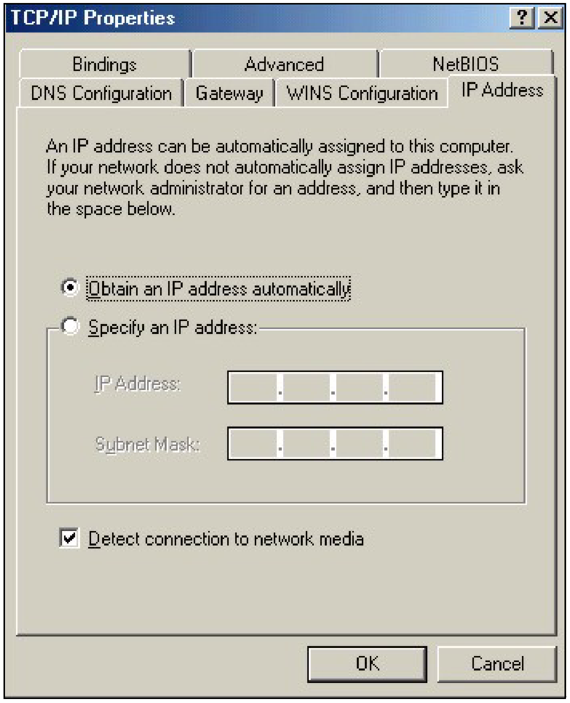
## Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 429** Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
?
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
IP Address:
Subnet Mask:
OK
Cancel

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

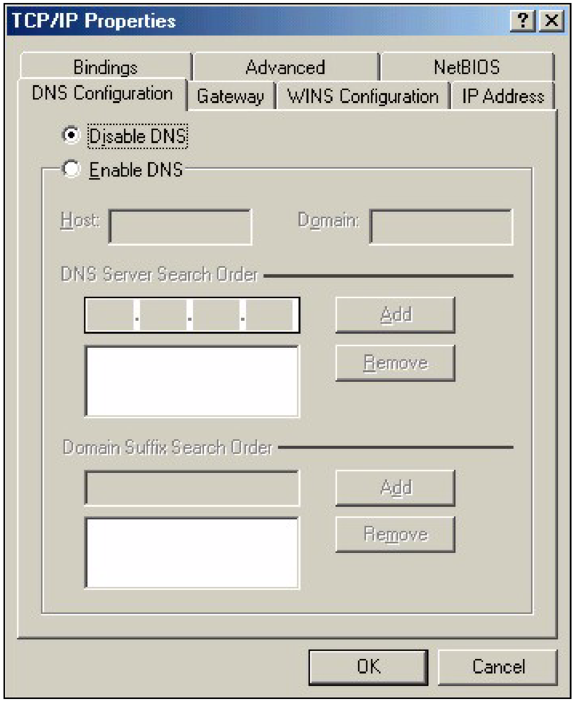
○ Specify an IP address:

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 430** Windows 95/98/Me: TCP/IP Properties: DNS Configuration


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
Host:
Domain:
DNS Server Search Order
Add
Remove
Domain Suffix Search Order
Add
Remove
OK
Cancel

● Disable DNS
○ Enable DNS

4 Click the **Gateway** tab.
   - If you do not know your gateway's IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
5 Click **OK** to save and close the **TCP/IP Properties** window.
6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7 Turn on your ZyWALL and restart your computer when prompted.

### Verifying Settings

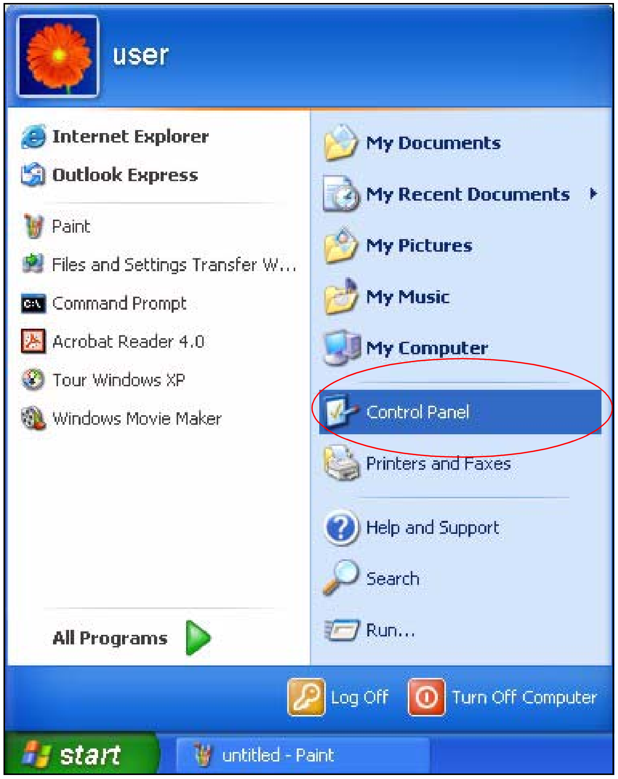
1 Click **Start** and then **Run**.
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

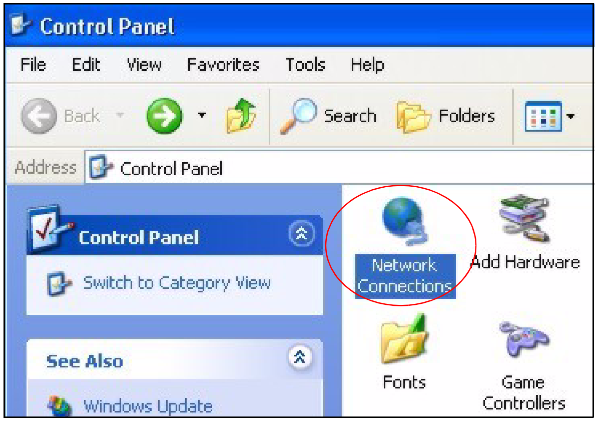
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 431** Windows XP: Start Menu


user
Internet Explorer
Outlook Express
Paint
Files and Settings Transfer W...
Command Prompt
Acrobat Reader 4.0
Tour Windows XP
Windows Movie Maker
All Programs
My Documents
My Recent Documents
My Pictures
My Music
My Computer
Control Panel
Printers and Faxes
Help and Support
Search
Run...
Log Off
Turn Off Computer
start
untitled - Paint

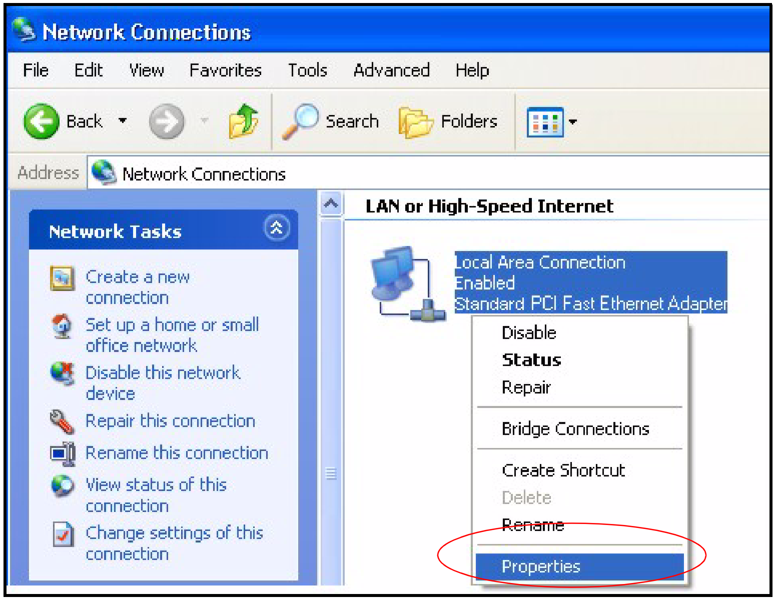
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

**Figure 432** Windows XP: Control Panel


Control Panel
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
Control Panel
Control Panel
Switch to Category View
See Also
Windows Update
Network Connections
Add Hardware
Fonts
Game Controllers

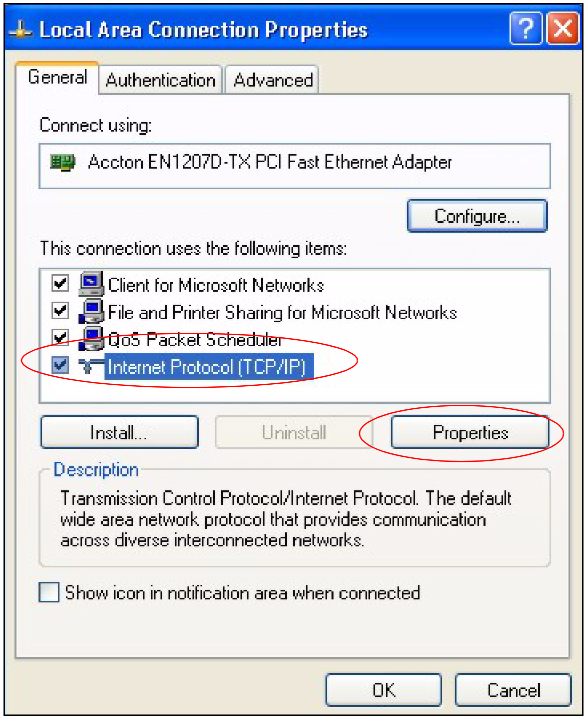
3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 433** Windows XP: Control Panel: Network Connections: Properties


Network Connections
File Edit View Favorites Tools Advanced Help
Back
Search
Folders
Address
Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

**Figure 434** Windows XP: Local Area Connection Properties

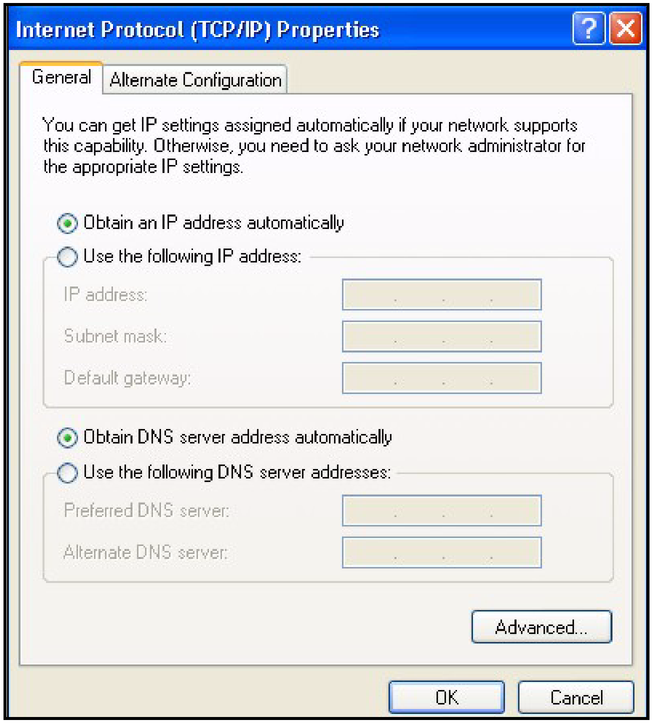

Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
☐ Show icon in notification area when connected
OK
Cancel

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

**Figure 435** Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

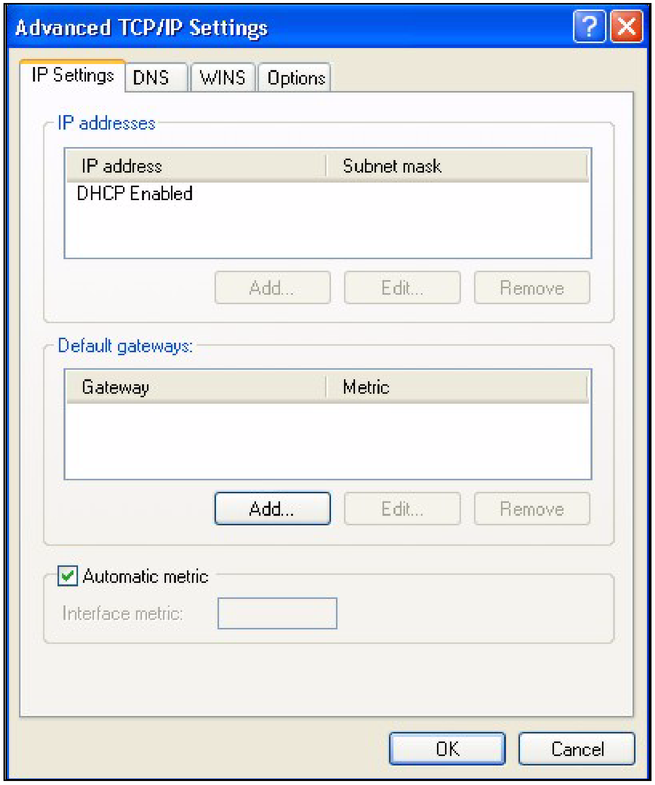
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

**Figure 436** Windows XP: Advanced TCP/IP Properties

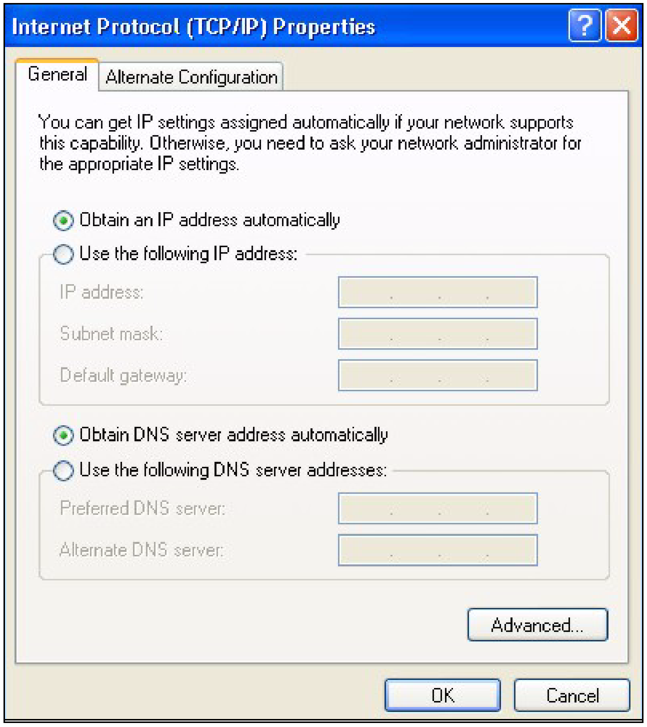

Advanced TCP/IP Settings
IP Settings
DNS
WINS
Options
IP addresses
IP address
Subnet mask
DHCP Enabled
Add...
Edit...
Remove
Default gateways:
Gateway
Metric
Add...
Edit...
Remove
☑ Automatic metric
Interface metric:
OK
Cancel

7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 437** Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ZyWALL and restart your computer (if prompted).

### Verifying Settings

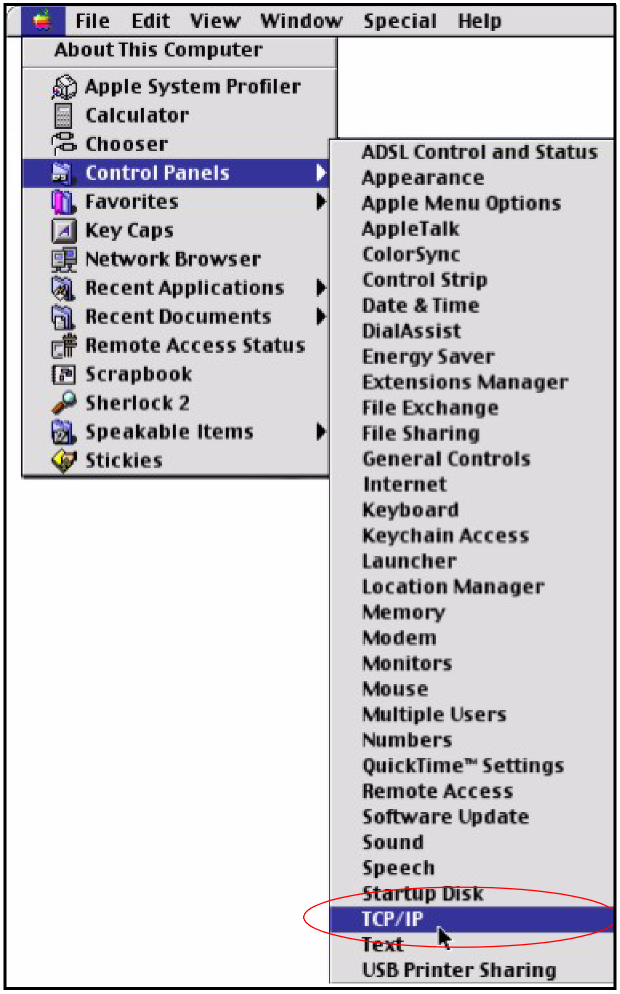
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

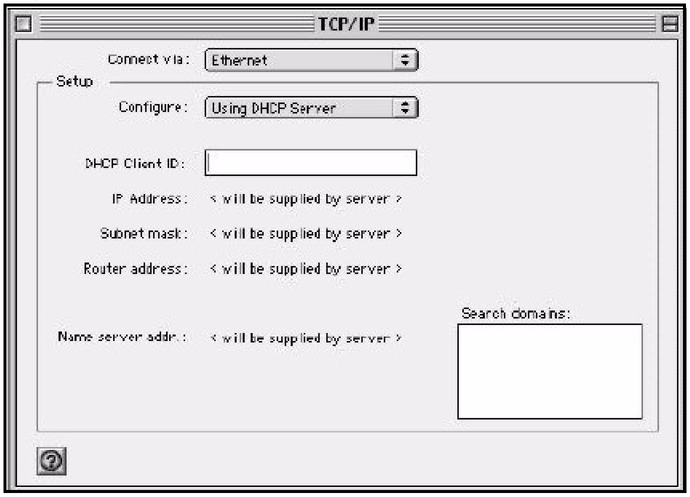
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 438** Macintosh OS 8/9: Apple Menu


File
Edit
View
Window
Special
Help
About This Computer
Apple System Profiler
Calculator
Chooser
Control Panels
Favorites
Key Caps
Network Browser
Recent Applications
Recent Documents
Remote Access Status
Scrapbook
Sherlock 2
Speakable Items
Stickies
ADSL Control and Status
Appearance
Apple Menu Options
AppleTalk
ColorSync
Control Strip
Date & Time
DialAssist
Energy Saver
Extensions Manager
File Exchange
File Sharing
General Controls
Internet
Keyboard
Keychain Access
Launcher
Location Manager
Memory
Modem
Monitors
Mouse
Multiple Users
Numbers
QuickTime™ Settings
Remote Access
Software Update
Sound
Speech
Startup Disk
TCP/IP
Text
USB Printer Sharing

2 Select **Ethernet built-in** from the **Connect via** list.

**Figure 439** Macintosh OS 8/9: TCP/IP


TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyWALL in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyWALL and restart your computer (if prompted).

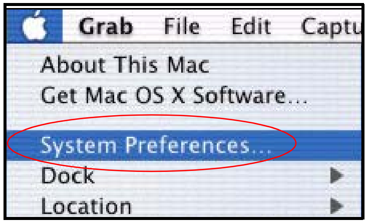
### Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

## Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 440** Macintosh OS X: Apple Menu

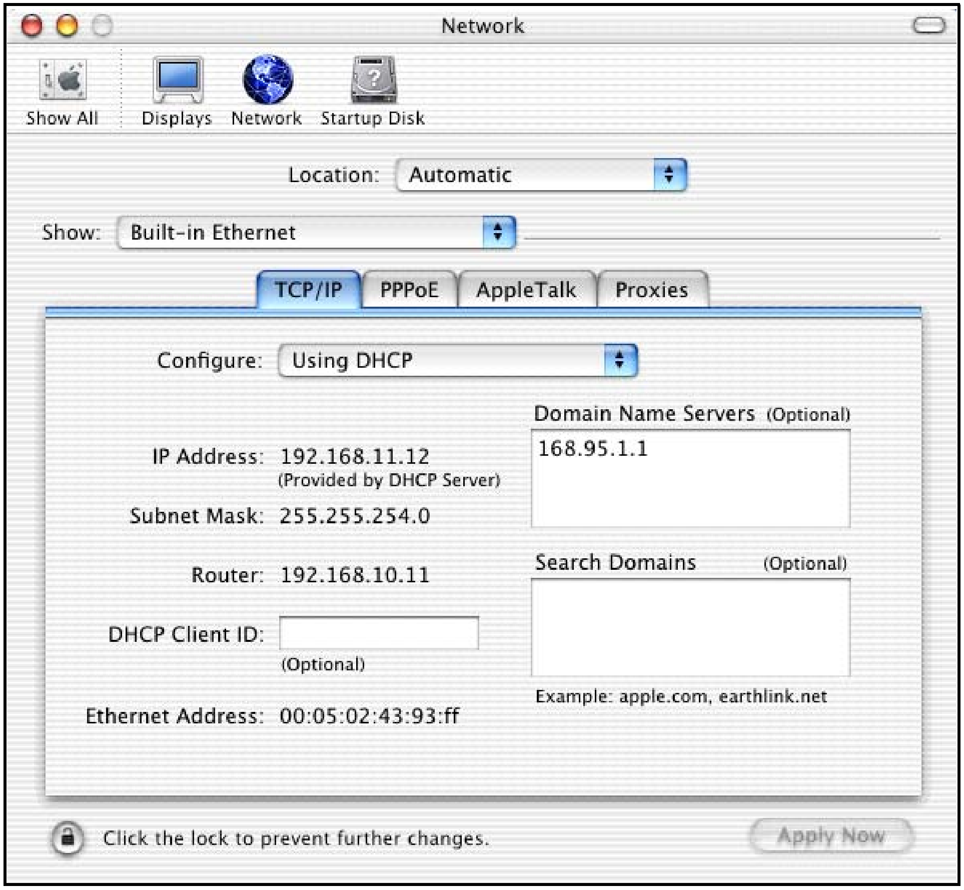

Grab
File
Edit
Captu
About This Mac
Get Mac OS X Software...
System Preferences...
Dock
Location

2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 441** Macintosh OS X: Network



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your ZyWALL in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyWALL and restart your computer (if prompted).

### Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer’s TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

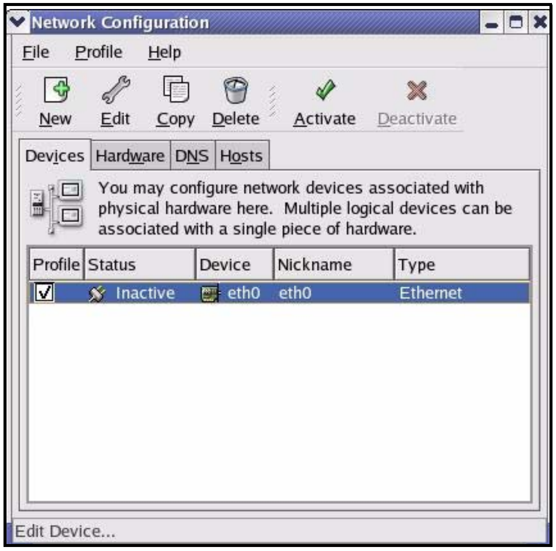
Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 442** Red Hat 9.0: KDE: Network Configuration: Devices

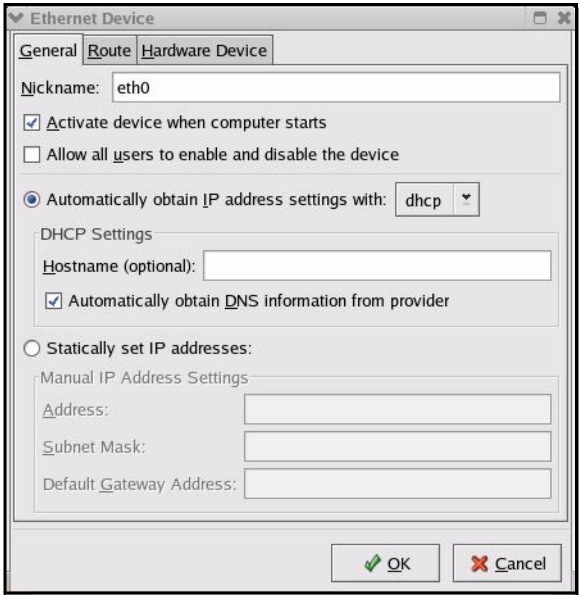

Network Configuration
File
Profile
Help
New
Edit
Copy
Delete
Activate
Deactivate
Devices
Hardware
DNS
Hosts
Edit Device...

You may configure network devices associated with physical hardware here. Multiple logical devices can be associated with a single piece of hardware.

| Profile | Status | Device | Nickname | Type |
|---|---|---|---|---|
| ☑ | Inactive | eth0 | eth0 | Ethernet |

2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 443** Red Hat 9.0: KDE: Ethernet Device: General


Ethernet Device
General
Route
Hardware Device
OK
Cancel

Nickname: eth0

☑ Activate device when computer starts

☐ Allow all users to enable and disable the device

● Automatically obtain IP address settings with: dhcp

DHCP Settings

Hostname (optional):

☑ Automatically obtain DNS information from provider

○ Statically set IP addresses:

Manual IP Address Settings

Address:

Subnet Mask:

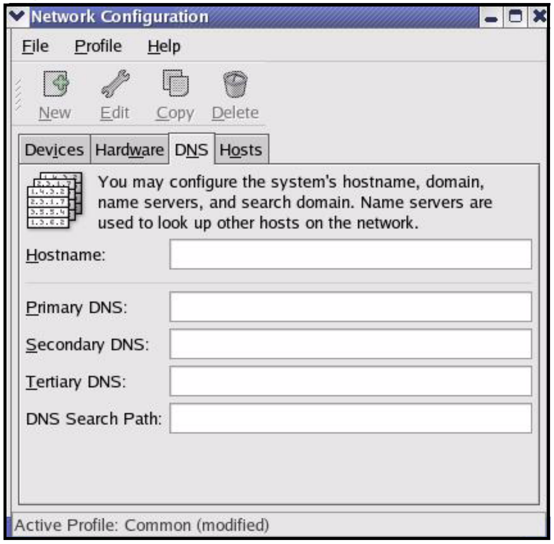
Default Gateway Address:

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

**Figure 444** Red Hat 9.0: KDE: Network Configuration: DNS



You may configure the system's hostname, domain, name servers, and search domain. Name servers are used to look up other hosts on the network.

Hostname:

Primary DNS:

Secondary DNS:

Tertiary DNS:

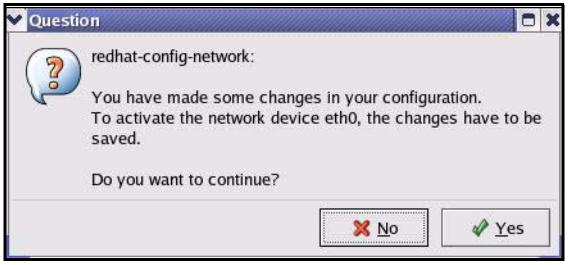
DNS Search Path:

Active Profile: Common (modified)

5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

**Figure 445** Red Hat 9.0: KDE: Network Configuration: Activate



redhat-config-network:

You have made some changes in your configuration. To activate the network device eth0, the changes have to be saved.

Do you want to continue?

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 446** Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 447** Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 448** Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.16.5.1
nameserver 172.16.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

**Figure 449** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

## Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 450** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.16.19.129  Bcast:172.16.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

# B

# Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

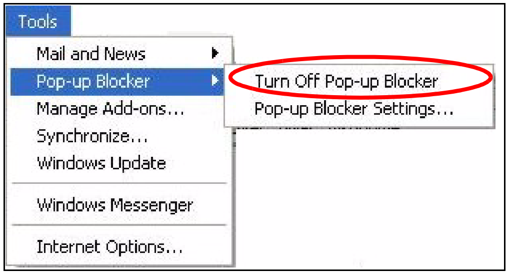
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

### Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 451** Pop-up Blocker

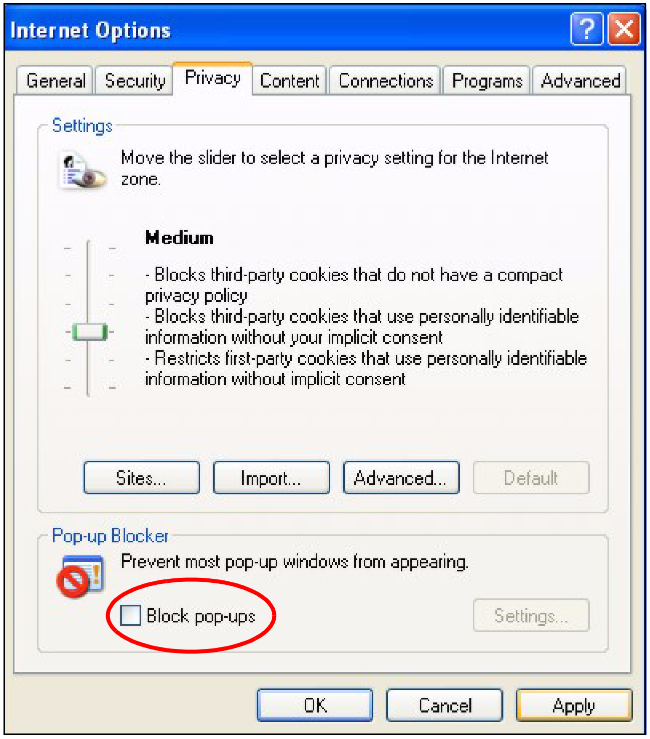

Tools
Mail and News
Pop-up Blocker
Manage Add-ons...
Synchronize...
Windows Update
Windows Messenger
Internet Options...
Turn Off Pop-up Blocker
Pop-up Blocker Settings...

You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 452** Internet Options: Privacy


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Sites...
Import...
Advanced...
Default
Pop-up Blocker
Settings...
OK
Cancel
Apply

Move the slider to select a privacy setting for the Internet zone.

**Medium**

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

☐ Block pop-ups

3 Click **Apply** to save this setting.

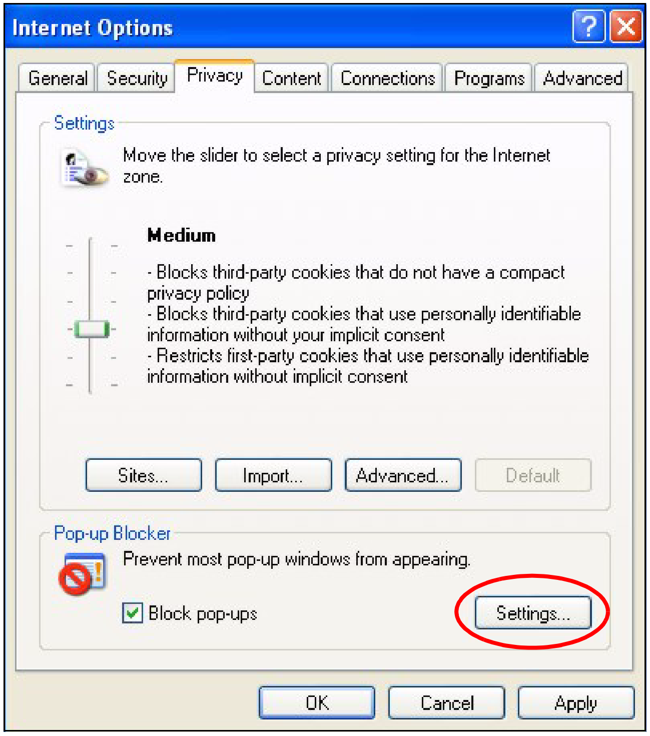
## Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

**Figure 453** Internet Options: Privacy


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Sites...
Import...
Advanced...
Default
Pop-up Blocker
Settings...
OK
Cancel
Apply

Move the slider to select a privacy setting for the Internet zone.

**Medium**

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

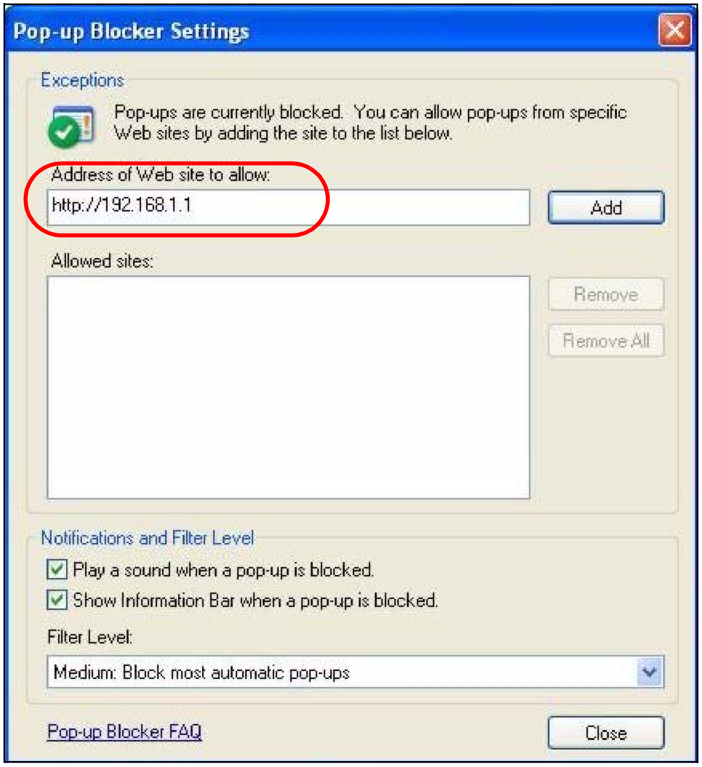
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 454** Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Pop-up Blocker FAQ
Close

Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow:
http://192.168.1.1

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level:
Medium: Block most automatic pop-ups

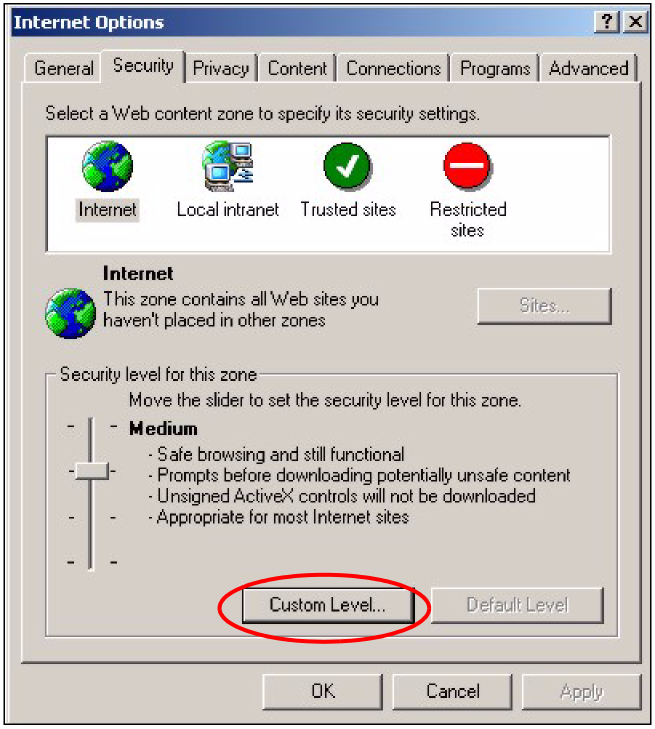
5 Click **Close** to return to the **Privacy** screen.
6 Click **Apply** to save this setting.

## JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

**Figure 455** Internet Options: Security



Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Internet
Local intranet
Trusted sites
Restricted sites
Sites...
Security level for this zone
Custom Level...
Default Level
OK
Cancel
Apply

Select a Web content zone to specify its security settings.

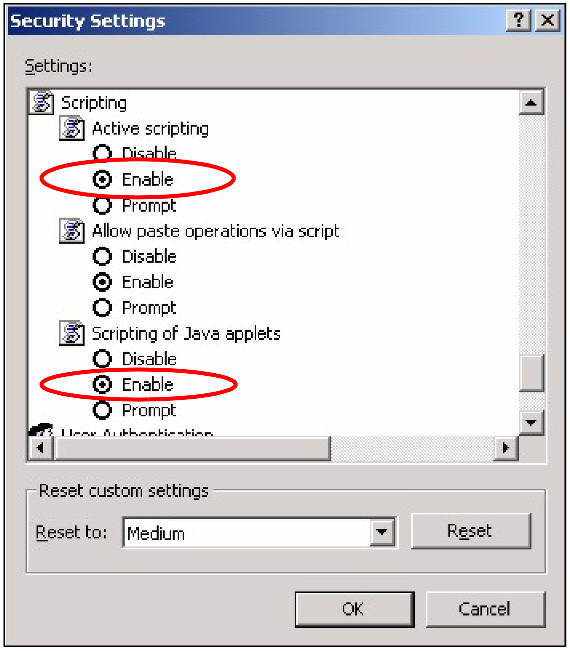
**Internet**
This zone contains all Web sites you haven't placed in other zones

Move the slider to set the security level for this zone.

**Medium**
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.
3 Scroll down to **Scripting**.
4 Under **Active scripting** make sure that **Enable** is selected (the default).
5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
6 Click **OK** to close the window.

**Figure 456** Security Settings - Java Scripting

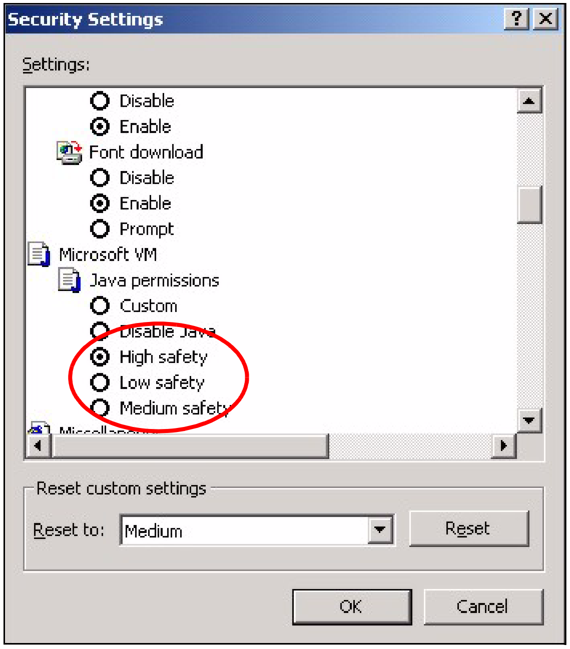

Security Settings
Settings:
Reset custom settings
Reset to:
Medium
Reset
OK
Cancel

Scripting
Active scripting
○ Disable
● Enable
○ Prompt
Allow paste operations via script
○ Disable
● Enable
○ Prompt
Scripting of Java applets
○ Disable
● Enable
○ Prompt

## Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

**Figure 457** Security Settings - Java

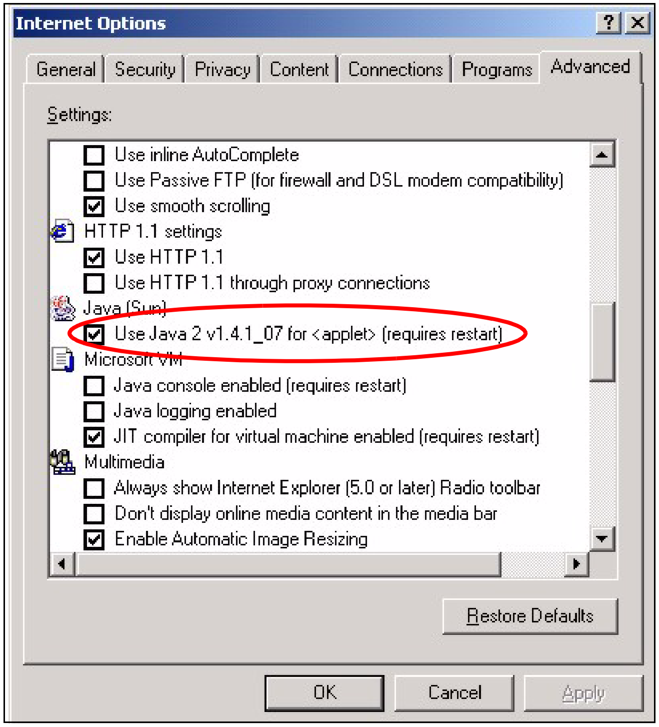

Security Settings
Settings:
Reset custom settings
Reset to:
Medium
Reset
OK
Cancel

○ Disable
● Enable
Font download
○ Disable
● Enable
○ Prompt
Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety

### JAVA (Sun)

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2. Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3. Click **OK** to close the window.

**Figure 458** Java (Sun)


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings:
Restore Defaults
OK
Cancel
Apply

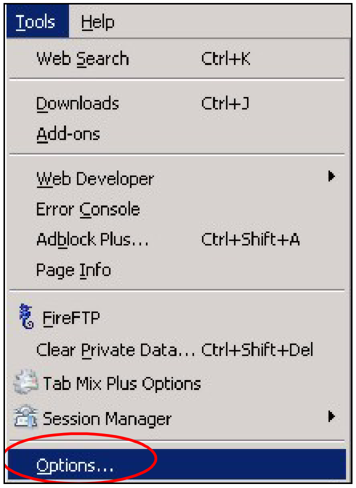
☐ Use inline AutoComplete
☐ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
☐ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
☐ Java console enabled (requires restart)
☐ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
☐ Always show Internet Explorer (5.0 or later) Radio toolbar
☐ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

## Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

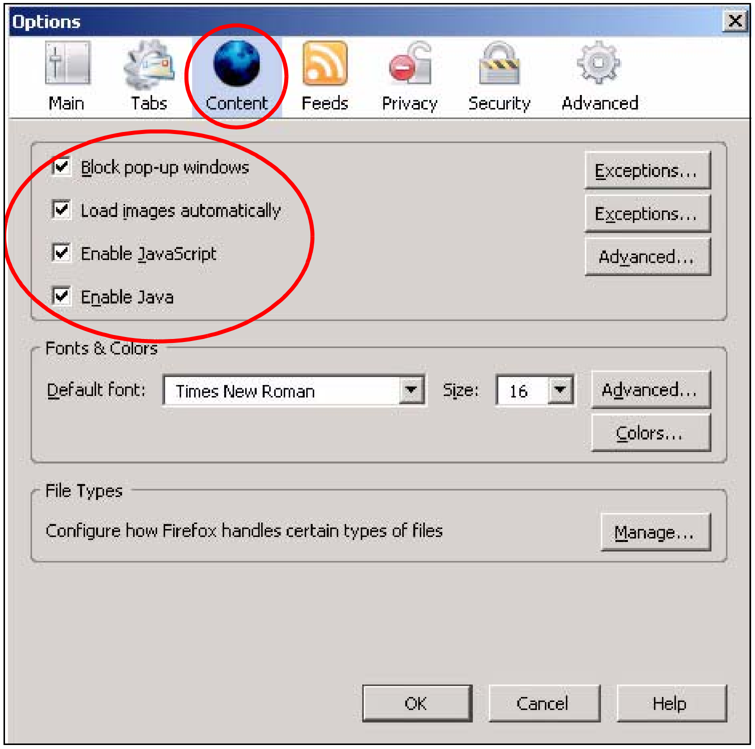
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

**Figure 459** Mozilla Firefox: Tools > Options


Tools
Help
Web Search Ctrl+K
Downloads Ctrl+J
Add-ons
Web Developer
Error Console
Adblock Plus... Ctrl+Shift+A
Page Info
FireFTP
Clear Private Data... Ctrl+Shift+Del
Tab Mix Plus Options
Session Manager
Options...

Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

**Figure 460** Mozilla Firefox Content Security


Options
Main
Tabs
Content
Feeds
Privacy
Security
Advanced
Exceptions...
Exceptions...
Advanced...
Advanced...
Colors...
Manage...
OK
Cancel
Help

☑ Block pop-up windows
☑ Load images automatically
☑ Enable JavaScript
☑ Enable Java

Fonts & Colors
Default font: Times New Roman
Size: 16

File Types
Configure how Firefox handles certain types of files

# C

# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

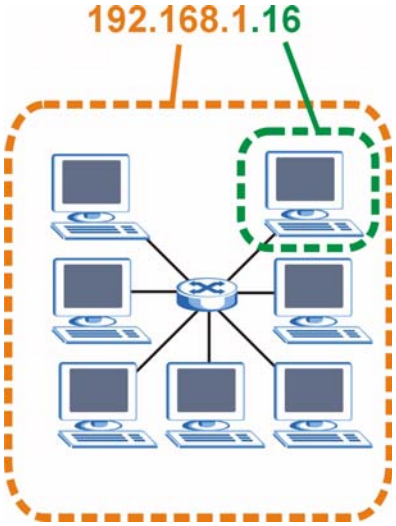
## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 461** Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 227** IP Address Network Number and Host ID Example

| | 1ST OCTET: (192) | 2ND OCTET: (168) | 3RD OCTET: (1) | 4TH OCTET (2) |
|---|---|---|---|---|
| IP Address (Binary) | 11000000 | 10101000 | 00000001 | 00000010 |
| Subnet Mask (Binary) | **11111111** | **11111111** | **11111111** | 00000000 |
| Network Number | **11000000** | **10101000** | **00000001** | |
| Host ID | | | | 00000010 |

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 228** Subnet Masks

| | BINARY | | | | DECIMAL |
|---|---|---|---|---|---|
| | 1ST OCTET | 2ND OCTET | 3RD OCTET | 4TH OCTET | |
| 8-bit mask | 11111111 | 00000000 | 00000000 | 00000000 | 255.0.0.0 |
| 16-bit mask | 11111111 | 11111111 | 00000000 | 00000000 | 255.255.0.0 |
| 24-bit mask | 11111111 | 11111111 | 11111111 | 00000000 | 255.255.255.0 |
| 29-bit mask | 11111111 | 11111111 | 11111111 | 11111000 | 255.255.255.248 |

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 229** Maximum Host Numbers

| SUBNET MASK | | HOST ID SIZE | | MAXIMUM NUMBER OF HOSTS |
|---|---|---|---|---|
| 8 bits | 255.0.0.0 | 24 bits | $2^{24} – 2$ | 16777214 |
| 16 bits | 255.255.0.0 | 16 bits | $2^{16} – 2$ | 65534 |
| 24 bits | 255.255.255.0 | 8 bits | $2^{8} – 2$ | 254 |
| 29 bits | 255.255.255.248 | 3 bits | $2^{3} – 2$ | 6 |

# Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 230** Alternative Subnet Mask Notation

| SUBNET MASK | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|---|---|---|---|
| 255.255.255.0 | /24 | 0000 0000 | 0 |
| 255.255.255.128 | /25 | 1000 0000 | 128 |

**Table 230** Alternative Subnet Mask Notation (continued)

| SUBNET MASK | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|---|---|---|---|
| 255.255.255.192 | /26 | 1100 0000 | 192 |
| 255.255.255.224 | /27 | 1110 0000 | 224 |
| 255.255.255.240 | /28 | 1111 0000 | 240 |
| 255.255.255.248 | /29 | 1111 1000 | 248 |
| 255.255.255.252 | /30 | 1111 1100 | 252 |

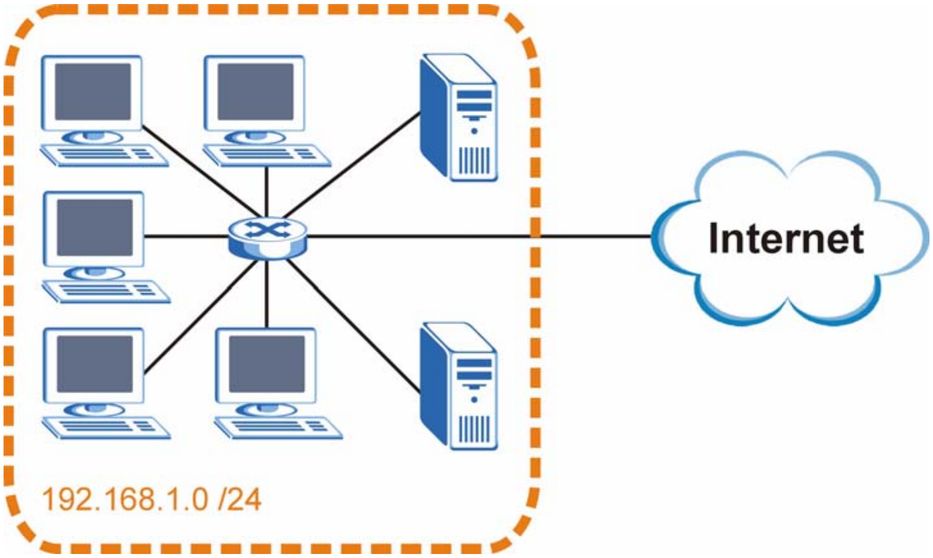
# Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 462** Subnetting Example: Before Subnetting

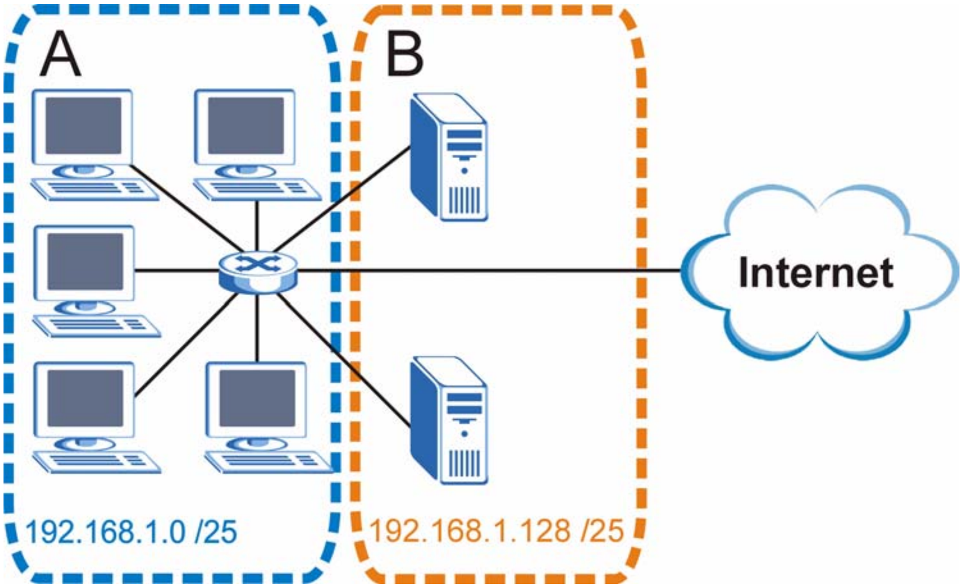


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 463** Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving $2^6$ - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 231** Subnet 1

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address (Decimal) | 192.168.1. | 0 |
| IP Address (Binary) | 11000000.10101000.00000001. | **00**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.0 | Lowest Host ID: 192.168.1.1 | |
| Broadcast Address: 192.168.1.63 | Highest Host ID: 192.168.1.62 | |

**Table 232** Subnet 2

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 64 |
| IP Address (Binary) | 11000000.10101000.00000001. | **01**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.64 | Lowest Host ID: 192.168.1.65 | |
| Broadcast Address: 192.168.1.127 | Highest Host ID: 192.168.1.126 | |

**Table 233** Subnet 3

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 128 |
| IP Address (Binary) | 11000000.10101000.00000001. | **10**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.128 | Lowest Host ID: 192.168.1.129 | |
| Broadcast Address: 192.168.1.191 | Highest Host ID: 192.168.1.190 | |

**Table 234** Subnet 4

| IP/SUBNET MASK | NETWORK NUMBER | LAST OCTET BIT VALUE |
|---|---|---|
| IP Address | 192.168.1. | 192 |
| IP Address (Binary) | 11000000.10101000.00000001. | **11**000000 |
| Subnet Mask (Binary) | 11111111.11111111.11111111. | **11**000000 |
| Subnet Address: 192.168.1.192 | Lowest Host ID: 192.168.1.193 | |
| Broadcast Address: 192.168.1.255 | Highest Host ID: 192.168.1.254 | |

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 235** Eight Subnets

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 1 | 0 | 1 | 30 | 31 |
| 2 | 32 | 33 | 62 | 63 |
| 3 | 64 | 65 | 94 | 95 |
| 4 | 96 | 97 | 126 | 127 |

**Table 235** Eight Subnets (continued)

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|---|---|---|---|---|
| 5 | 128 | 129 | 158 | 159 |
| 6 | 160 | 161 | 190 | 191 |
| 7 | 192 | 193 | 222 | 223 |
| 8 | 224 | 225 | 254 | 255 |

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 236** 24-bit Network Number Subnet Planning

| NO. “BORROWED” HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.255.128 (/25) | 2 | 126 |
| 2 | 255.255.255.192 (/26) | 4 | 62 |
| 3 | 255.255.255.224 (/27) | 8 | 30 |
| 4 | 255.255.255.240 (/28) | 16 | 14 |
| 5 | 255.255.255.248 (/29) | 32 | 6 |
| 6 | 255.255.255.252 (/30) | 64 | 2 |
| 7 | 255.255.255.254 (/31) | 128 | 1 |

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 237** 16-bit Network Number Subnet Planning

| NO. “BORROWED” HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 1 | 255.255.128.0 (/17) | 2 | 32766 |
| 2 | 255.255.192.0 (/18) | 4 | 16382 |
| 3 | 255.255.224.0 (/19) | 8 | 8190 |
| 4 | 255.255.240.0 (/20) | 16 | 4094 |
| 5 | 255.255.248.0 (/21) | 32 | 2046 |
| 6 | 255.255.252.0 (/22) | 64 | 1022 |
| 7 | 255.255.254.0 (/23) | 128 | 510 |
| 8 | 255.255.255.0 (/24) | 256 | 254 |
| 9 | 255.255.255.128 (/25) | 512 | 126 |
| 10 | 255.255.255.192 (/26) | 1024 | 62 |
| 11 | 255.255.255.224 (/27) | 2048 | 30 |
| 12 | 255.255.255.240 (/28) | 4096 | 14 |
| 13 | 255.255.255.248 (/29) | 8192 | 6 |

**Table 237** 16-bit Network Number Subnet Planning (continued)

| NO. “BORROWED” HOST BITS | SUBNET MASK | NO. SUBNETS | NO. HOSTS PER SUBNET |
|---|---|---|---|
| 14 | 255.255.255.252 (/30) | 16384 | 2 |
| 15 | 255.255.255.254 (/31) | 32768 | 1 |

# Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyWALL.

Once you have decided on the network number, pick an IP address for your ZyWALL that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyWALL will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyWALL unless you are instructed to do otherwise.

## Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

# D

# Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s**) is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
    - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
    - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 238** Commonly Used Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM/New-ICQ | TCP | 5190 | AOL's Internet Messenger service. It is also used as a listening port by ICQ. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP<br>UDP | 7648<br>24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers. |
| ESP (IPSEC_TUNNEL) | User-Defined | 50 | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| FINGER | TCP | 79 | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP | TCP<br>TCP | 20<br>21 | File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |
| HTTP | TCP | 80 | Hyper Text Transfer Protocol - a client/ server protocol for the world wide web. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic or routing purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |
| NFS | UDP | 2049 | Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments. |

**Table 238** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| RTELNET | TCP | 107 | Remote Telnet. |
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP | TCP | 115 | Simple File Transfer Protocol. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |
| TACACS | UDP | 49 | Login Host Protocol used for (Terminal Access Controller Access Control System). |

**Table 238** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| TELNET | TCP | 23 | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| TFTP | UDP | 69 | Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). |
| VDOLIVE | TCP | 7000 | Another videoconferencing solution. |

# Importing Certificates

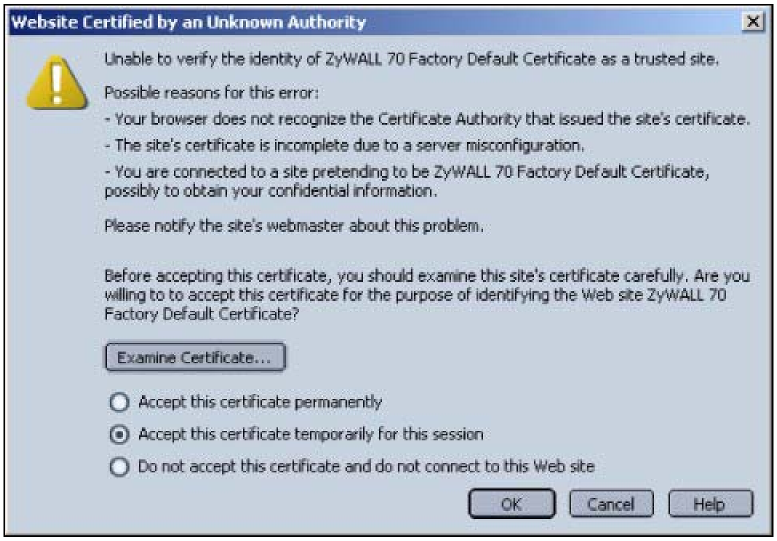
This appendix shows importing certificates examples using Internet Explorer 5.

## Import ZyWALL Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the ZyWALL's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

**Figure 464** Security Certificate



Website Certified by an Unknown Authority

Unable to verify the identity of ZyWALL 70 Factory Default Certificate as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be ZyWALL 70 Factory Default Certificate, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site ZyWALL 70 Factory Default Certificate?

○ Accept this certificate permanently
● Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this Web site

## Importing the ZyWALL's Certificate into Internet Explorer

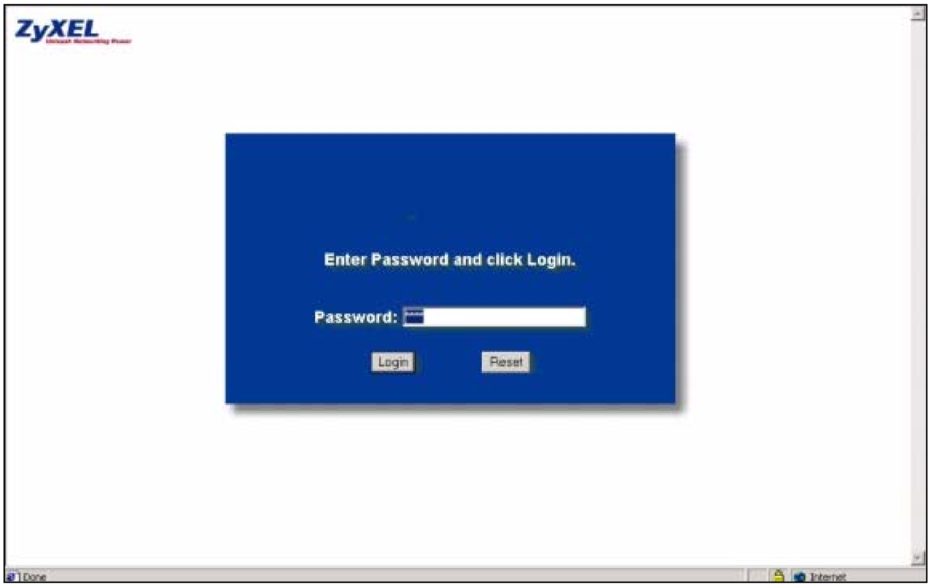
For Internet Explorer to trust a self-signed certificate from the ZyWALL, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a ZyWALL certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the ZyWALL's (self-signed) server certificate into your operating system as a trusted certification authority.

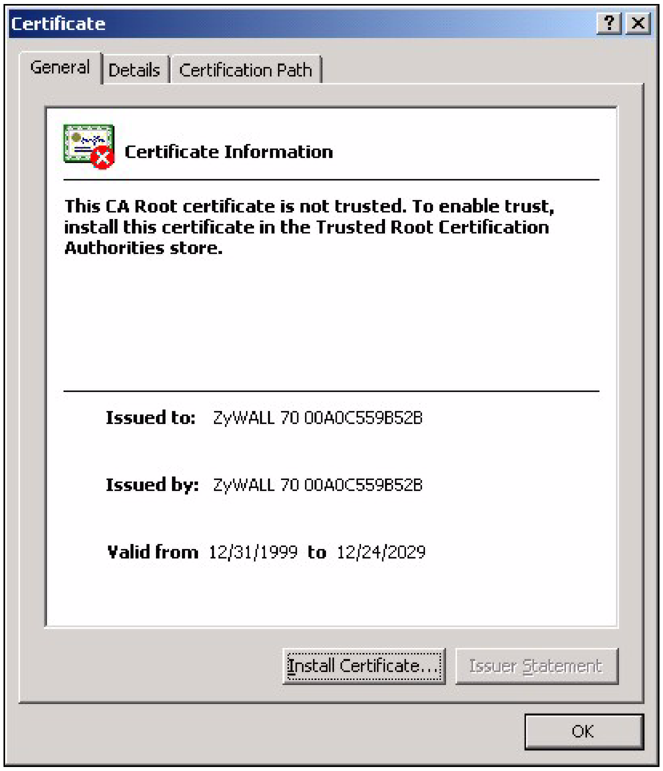
1 In Internet Explorer, double click the lock shown in the following screen.

**Figure 465** Login Screen


Enter Password and click Login.
Password:
Login
Reset
Done
Internet

2 Click **Install Certificate** to open the **Install Certificate** wizard.

**Figure 466** Certificate General Information before Import


Certificate
General
Details
Certification Path
Install Certificate...
Issuer Statement
OK

**Certificate Information**

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

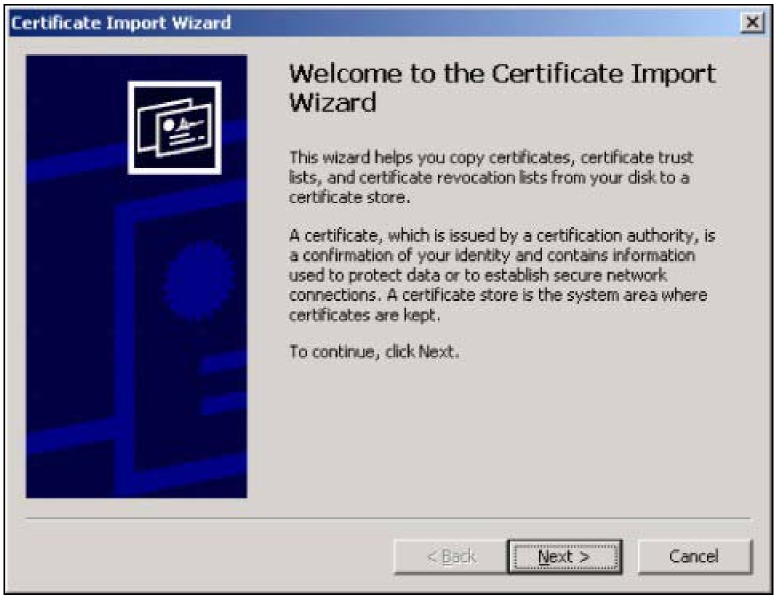
**Issued to:** ZyWALL 70 00A0C559B52B

**Issued by:** ZyWALL 70 00A0C559B52B

**Valid from** 12/31/1999 **to** 12/24/2029

3 Click **Next** to begin the **Install Certificate** wizard.

**Figure 467** Certificate Import Wizard 1



Welcome to the Certificate Import Wizard

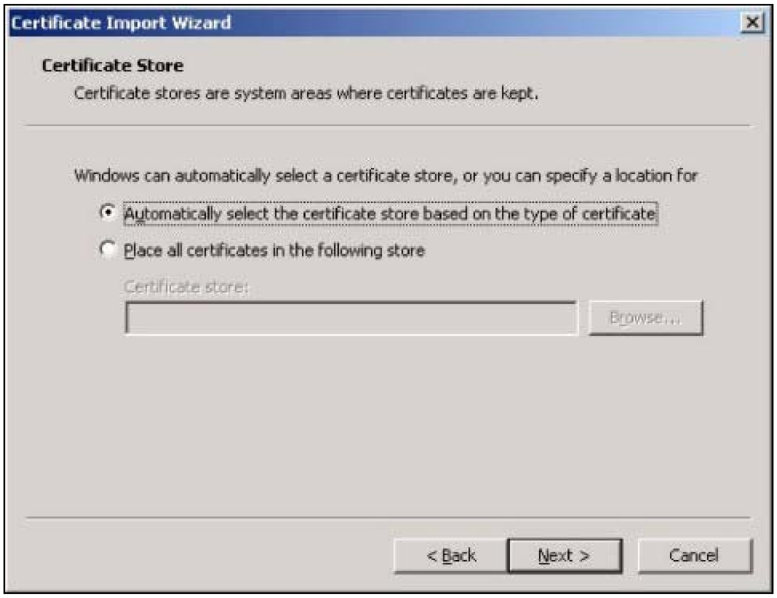
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4 Select where you would like to store the certificate and then click **Next**.

**Figure 468** Certificate Import Wizard 2



**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

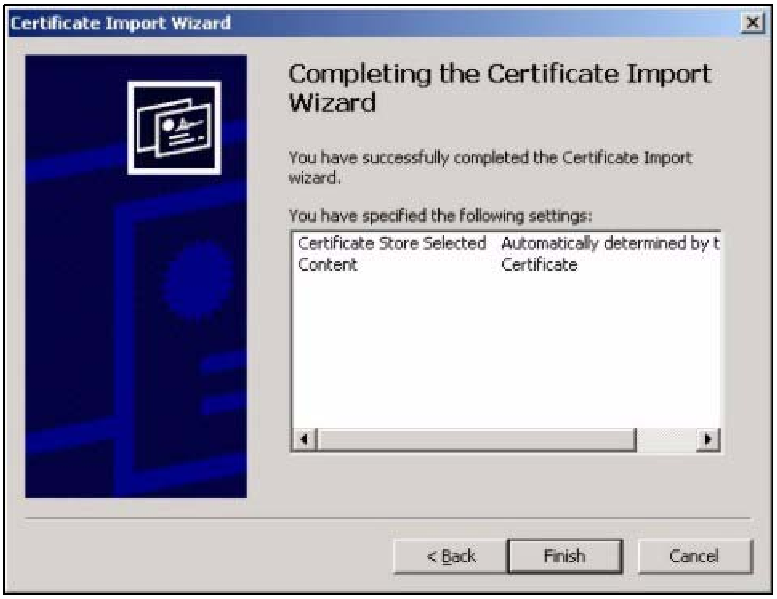
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5 Click **Finish** to complete the **Import Certificate** wizard.

**Figure 469** Certificate Import Wizard 3



Completing the Certificate Import Wizard

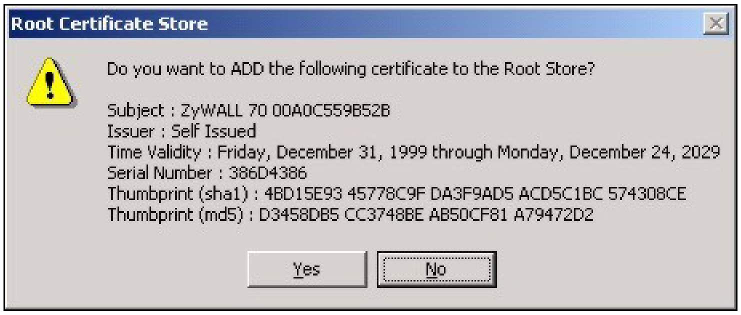
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected Automatically determined by t
Content Certificate

6 Click **Yes** to add the ZyWALL certificate to the root store.

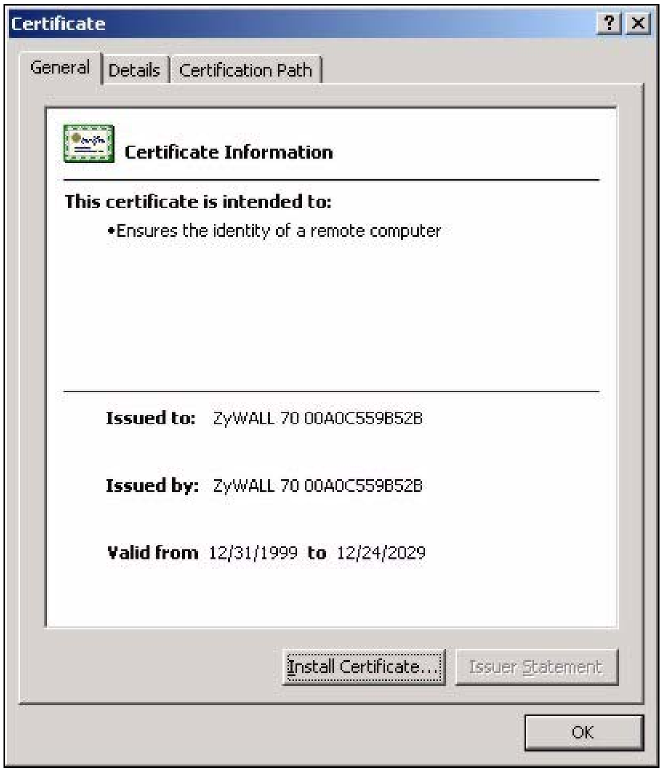
**Figure 470** Root Certificate Store



Do you want to ADD the following certificate to the Root Store?

Subject : ZyWALL 70 00A0C559B52B
Issuer : Self Issued
Time Validity : Friday, December 31, 1999 through Monday, December 24, 2029
Serial Number : 386D4386
Thumbprint (sha1) : 4BD15E93 45778C9F DA3F9AD5 ACD5C1BC 574308CE
Thumbprint (md5) : D3458DB5 CC3748BE AB50CF81 A79472D2

Figure 471 Certificate General Information after Import


Certificate
General
Details
Certification Path
Certificate Information
Install Certificate...
Issuer Statement
OK

This certificate is intended to:

- Ensures the identity of a remote computer

Issued to: ZyWALL 70 00A0C559B52B

Issued by: ZyWALL 70 00A0C559B52B

Valid from 12/31/1999 to 12/24/2029

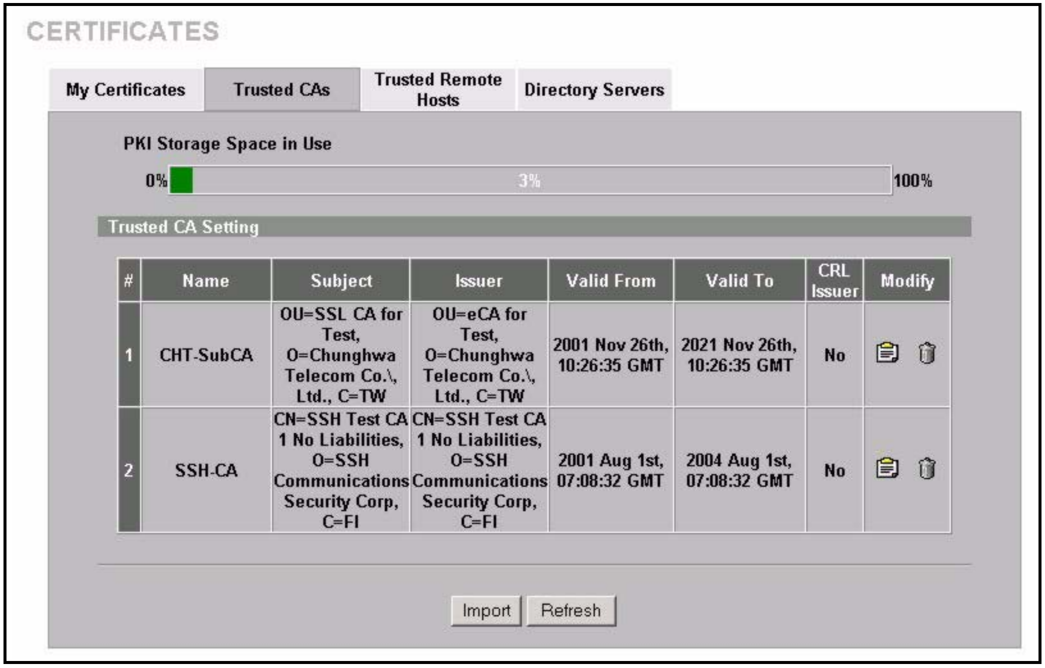
# Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyWALL.

You must have imported at least one trusted CA to the ZyWALL in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyWALL (see the ZyWALL’s **Trusted CA** web configurator screen).

**Figure 472** ZyWALL Trusted CA Screen


CERTIFICATES
My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers
PKI Storage Space in Use
0%
3%
100%
Trusted CA Setting
Import
Refresh

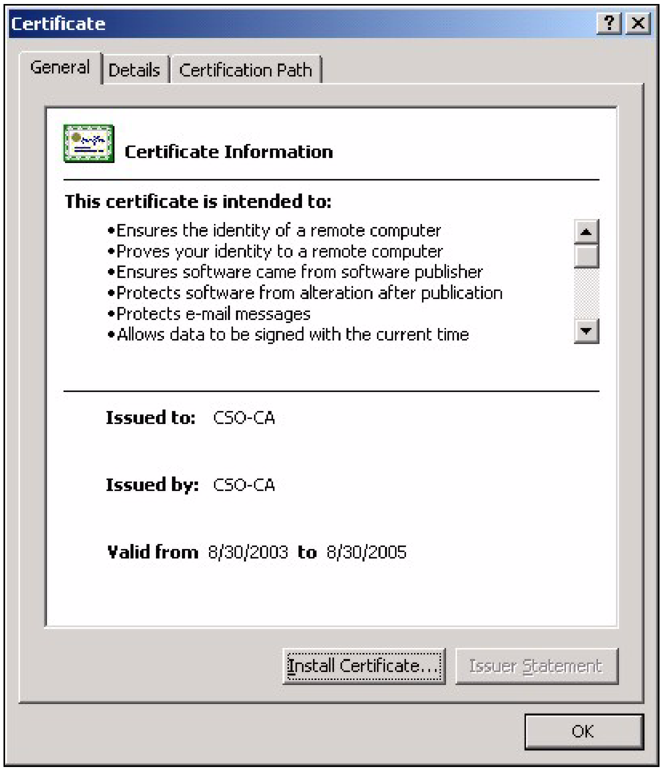
| # | Name | Subject | Issuer | Valid From | Valid To | CRL Issuer | Modify |
|---|---|---|---|---|---|---|---|
| 1 | CHT-SubCA | OU=SSL CA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW | OU=eCA for Test, O=Chunghwa Telecom Co.\, Ltd., C=TW | 2001 Nov 26th, 10:26:35 GMT | 2021 Nov 26th, 10:26:35 GMT | No | 📋 🗑 |
| 2 | SSH-CA | CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI | CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI | 2001 Aug 1st, 07:08:32 GMT | 2004 Aug 1st, 07:08:32 GMT | No | 📋 🗑 |

The CA sends you a package containing the CA’s trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

## Installing the CA’s Certificate

1 Double click the CA’s trusted certificate to produce a screen similar to the one shown next.

**Figure 473** CA Certificate Example



Certificate
General
Details
Certification Path
Certificate Information

**This certificate is intended to:**

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time

**Issued to:** CSO-CA

**Issued by:** CSO-CA

**Valid from** 8/30/2003 **to** 8/30/2005

Install Certificate...
Issuer Statement
OK

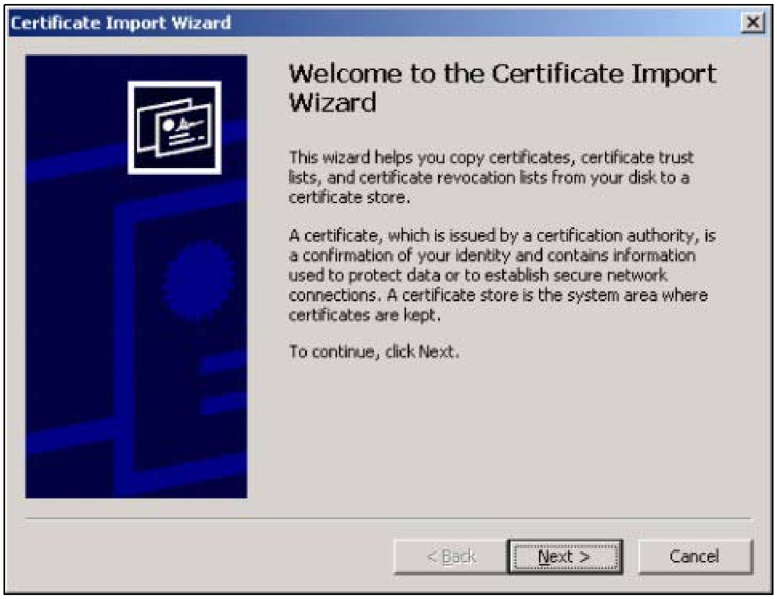
2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

## Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

**Figure 474** Personal Certificate Import Wizard 1



Certificate Import Wizard

Welcome to the Certificate Import Wizard

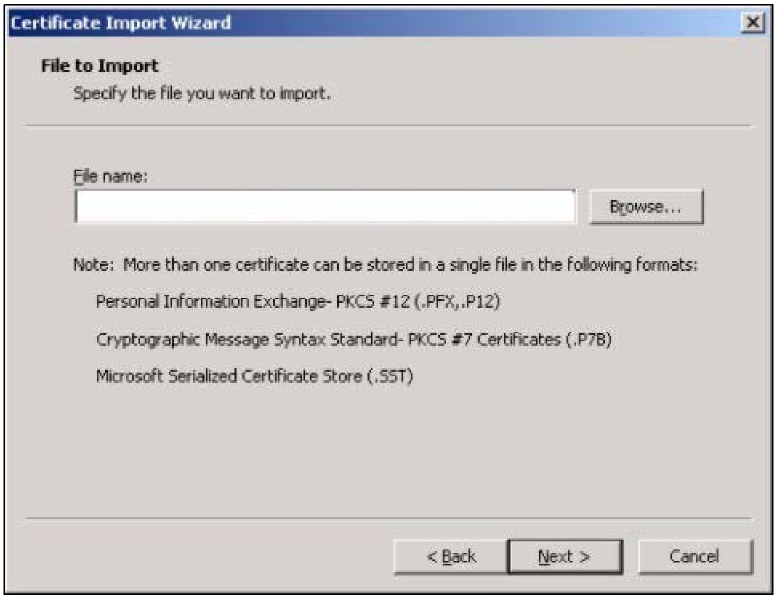
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

**Figure 475** Personal Certificate Import Wizard 2



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

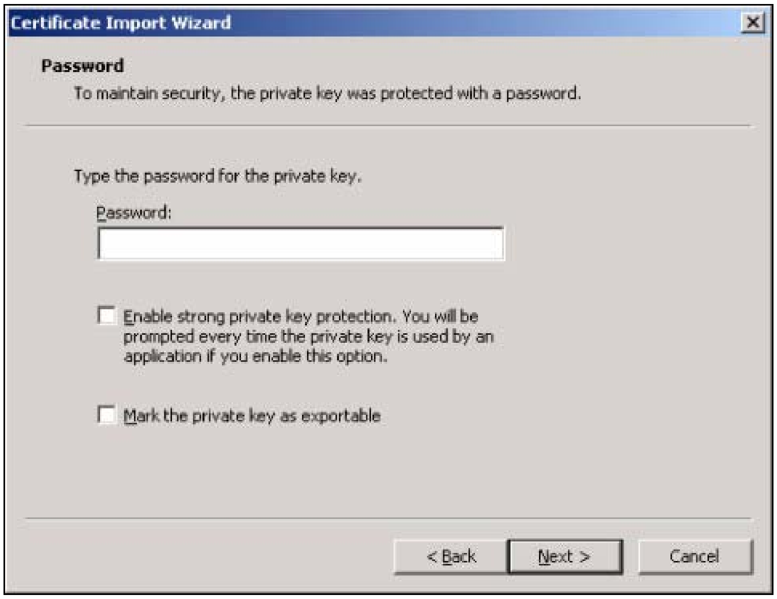
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

3 Enter the password given to you by the CA.

**Figure 476** Personal Certificate Import Wizard 3



**Password**

To maintain security, the private key was protected with a password.

Type the password for the private key.

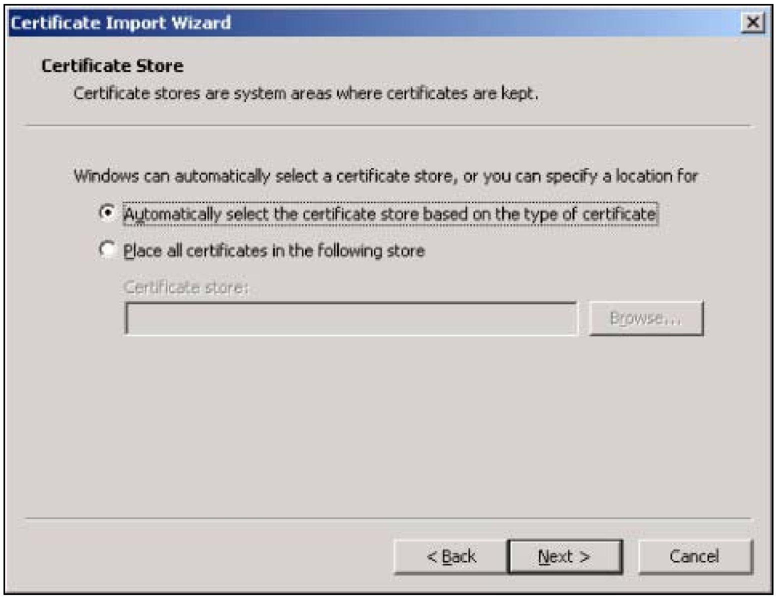
Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☐ Mark the private key as exportable

4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

**Figure 477** Personal Certificate Import Wizard 4



**Certificate Store**

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

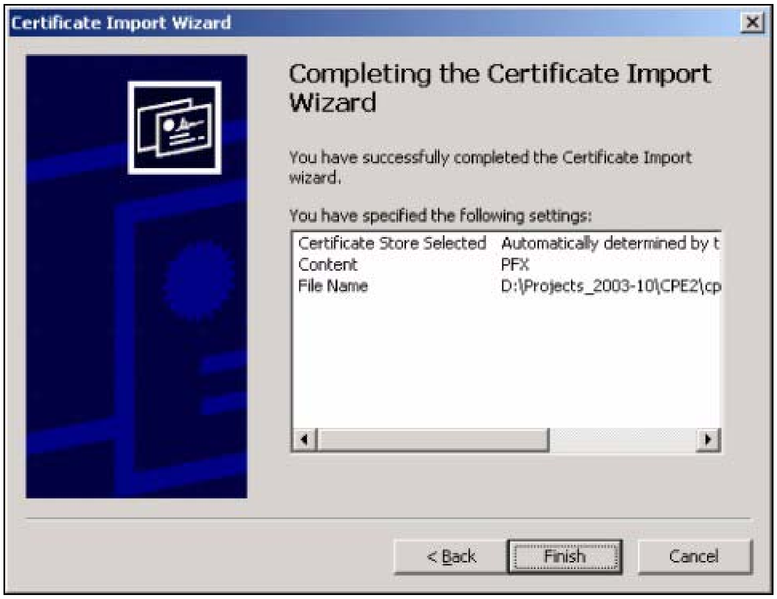
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

5 Click **Finish** to complete the wizard and begin the import process.

**Figure 478** Personal Certificate Import Wizard 5


Certificate Import Wizard
< Back
Finish
Cancel

Completing the Certificate Import Wizard

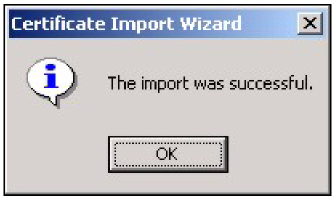
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

| | |
|---|---|
| Certificate Store Selected | Automatically determined by t |
| Content | PFX |
| File Name | D:\Projects_2003-10\CPE2\cp |

6 You should see the following screen when the certificate is correctly installed on your computer.

**Figure 479** Personal Certificate Import Wizard 6


Certificate Import Wizard
OK

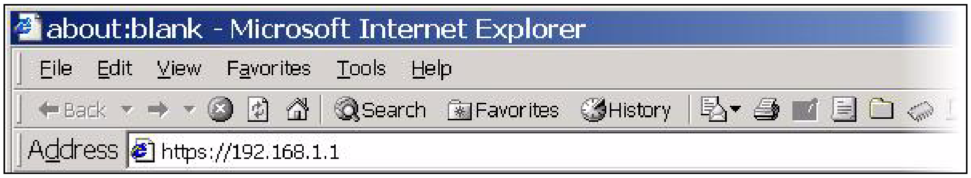
The import was successful.

## Using a Certificate When Accessing the ZyWALL Example

Use the following procedure to access the ZyWALL via HTTPS.

1 Enter 'https://ZyWALL IP Address/ in your browser's web address field.

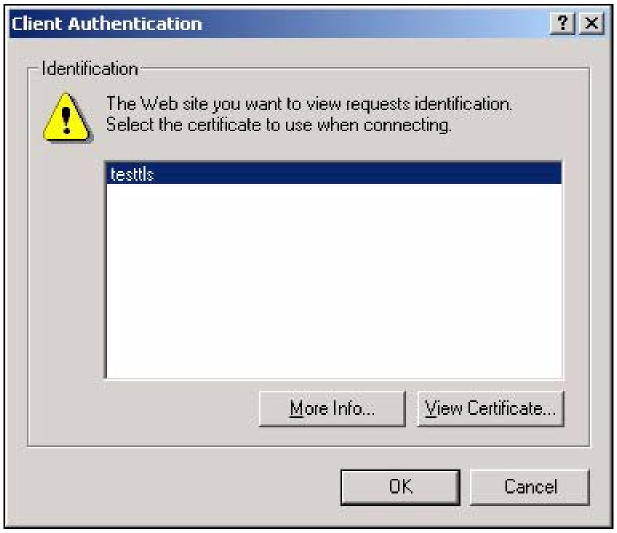
**Figure 480** Access the ZyWALL Via HTTPS


about:blank - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History

Address https://192.168.1.1

2 When **Authenticate Client Certificates** is selected on the ZyWALL, the following screen asks you to select a personal certificate to send to the ZyWALL. This screen displays even if you only have a single certificate as in the example.

**Figure 481** SSL Client Authentication

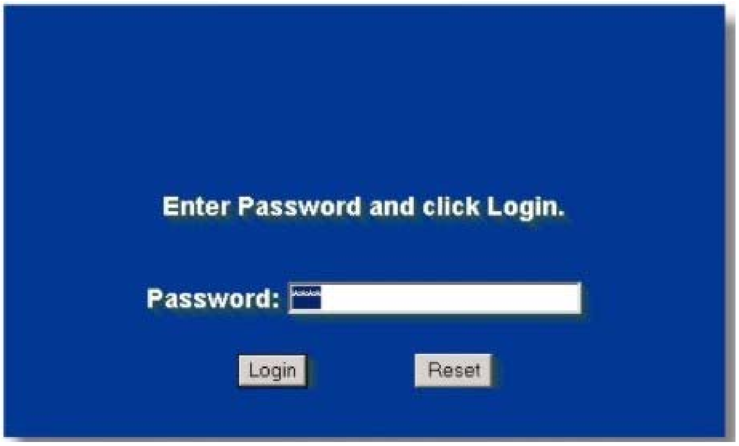


Client Authentication
Identification
testtls
More Info...
View Certificate...
OK
Cancel

The Web site you want to view requests identification.
Select the certificate to use when connecting.

**3** You next see the ZyWALL login screen.

**Figure 482** ZyWALL Secure Login Screen



Enter Password and click Login.

Password:
Login
Reset

# F

# Legal Information

## Copyright

Copyright © 2007 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

### Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

### Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

### Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of

ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

## Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

# G

# Customer Support

Please have the following information ready when you contact customer support.

## Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

## Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

## Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

## Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz

- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

### Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

### Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

### France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

### Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

### Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

### India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

### Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

### Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

### Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

### North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

### Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

### Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

### Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

### Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

### Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

### Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

### Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

### Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

### United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

# Index

## Numerics

9600 baud **467**

## A

active protocol **272**
  AH **272**
  and encapsulation **272**
  ESP **272**
Address Assignment **365**
address assignment **153**
AH **272**
  and transport mode **273**
ALG **411**
  RTP **412**
  SIP **413**
  STUN **413**
allocated budget **486**, **513**
alternative subnet mask notation **647**
anti-probing **211**
Application Layer Gateway. See ALG.
Applications **47**
  broadband connection **47**
applications **47**
asymmetrical routes **202**
  vs virtual interfaces **202**
AT command **483**, **572**
authentication **512**
authentication algorithms **257**, **263**
  and active protocol **257**
Authentication Header. See AH.
authentication protocol **486**, **512**

## B

backup configuration **460**, **572**
  TFTP **575**
bandwidth class **351**
bandwidth filter **351**
bandwidth management **351**
  address type **361**
  bandwidth borrowing **355**
  bandwidth class **351**
  bandwidth filter **351**, **360**
  class configuration **359**
  class setup **358**
  fairness-based scheduler **353**
  maximize bandwidth usage **353**, **358**
  monitor **363**
  priority-based scheduler **353**
  proportional allocation **352**
  root class **358**
  scheduler **353**, **358**
  statistics **362**
  sub-class layers **358**
baud **467**
BPDU **146**
bridge firewall **57**, **147**, **456**
Bridge Protocol Data Unit. See BPDU.
broadcast **135**
budget **513**
budget management **589**

## C

CA **295**
call back delay **485**
call control **589**
call history **590**
call scheduling **599**
  max number of schedule sets **599**
  PPPoE **601**
  precedence **599**
  setting up a schedule **600**
call-triggering packet **566**
certificate **267**
certificates **295**
  and IKE SA **259**
  CA **295**
  thumbprint algorithms **296**
  thumbprints **296**
  verifying fingerprints **296**
Certification Authority. See CA.
certifications **669**
  notices **670**
  viewing **670**
changing the password **472**

CHAP 486, 513

CNM 396

command interpreter mode 587

command line 573

commands
    FTP 573

computer names 136, 138

configuration backup 460, 572
    TFTP 575

configuration information 462

configuration restore 460, 577
    via console port 584

connection ID/name 514

console port 467, 561
    configuration upload 584
    data bits 467
    file backup 576
    file upload 583
    flow control 467
    parity 467
    restoring files 579
    settings 467
    speed 561, 562
    stop bit 467

contact information 673

content filter general 224

content filtering 223
    categories 223
    days and times 223
    filter list 223
    object 240
    policy 227
    restrict web features 223
    URL for blocked access 227

copyright 669

custom ports 216

customer support 673

## D

data bits 467

Data Terminal Ready. See DTR

date setting 449, 591

daylight saving 451, 592

Daytime time protocol 451

DDNS
    configuration 476, 477
    host 479
    offline 479
    type 479
    use server detected IP 479
    wildcard 479

default configuration 53

default server IP address 340

default settings 461

Denial of Service. See DoS.

device introduction 47

DHCP 65, 135, 136, 374, 493
    Relay 493
    Server 493
    WAN 568

DHCP clients 448

DHCP table 65

diagnostic 567

diagnostics 462

dial timeout 485

Diffie-Hellman key group 258
    Perfect Forward Secrecy (PFS) 273

Dimensions 613

disclaimer 669

DMZ
    IP alias setup 503
    port filter setup 501
    setup 501
    TCP/IP setup 502

DNS 395

DNS Server
    For VPN Host 366

DNS server address assignment 153

domain name 447, 562

Domain Name System. See DNS.

DoS 191, 214

drop timeout 485

DSL modem 511

DTR 168, 484

Dynamic DNS 374

Dynamic Host Configuration Protocol. See DHCP.

DYNDNS Wildcard 366, 374

## E

Encapsulating Security Payload. See ESP.

encapsulation 498, 510, 514
    and active protocol 272
    transport mode 272
    tunnel mode 272
    VPN 272

encryption algorithms 257, 263
    and active protocol 257

entering information 469

ESP 272
    and transport mode 273

ESSID **610**

Ethernet
  encapsulation **70**, **497**, **510**

extended authentication **260**

F

F/W version **562**

factory defaults **461**

factory-default configuration file **53**

FCC interference statement **669**

file backup
  console port **576**

file maintenance
  over WAN **574**

file upload
  console port **583**
  FTP **581**
  TFTP **582**
  Xmodem **583**

filename conventions **571**

filter **489**, **501**, **516**, **541**
  and NAT **552**
  applying **553**
  configuration **541**
  configuring **544**
  DMZ **554**
  example **550**
  filter rule execution **542**
  generic filter rule **549**
  incoming protocol **495**
  IP filter logic flow **548**
  protocol **495**
  remote node **555**
  structure **542**

firewall
  action for matched packets **211**
  activating **539**
  address type **210**, **230**
  anti-probing **211**
  creating/editing rules **208**
  custom ports **216**
  DoS **214**
  Dos threshold **214**
  maximum incomplete high **214**
  maximum incomplete low **214**
  one minute high **214**
  one minute low **214**
  rules **191**
  rules for VPN **89**, **93**
  service type **216**
  SMT menus **539**
  stateful inspection **191**
  TCP maximum incomplete **214**
  three-way handshake **212**
  threshold **213**
  VPN **93**
  when to use **553**

firmware
  file maintenance **571**
  upload **457**

firmware upload **579**
  FTP **580**

flow control **467**

FTP **374**, **391**
  commands **573**
  file upload **581**
  firmware upload **580**
  GUI-based clients **574**
  restoring files **577**

G

gateway IP address **498**, **515**, **520**

general setup **447**, **475**

GMT **451**

Greenwich Mean Time. See GMT.

H

H.323 **412**
  RTP **412**

Hello BPDU **147**

hidden menus **468**

HTTPS **378**
  example **380**

HyperTerminal **576**, **579**, **583**, **585**

I

IANA **134**, **652**

iCard **129**

idle timeout **486**, **512**, **513**

IGMP **135**, **136**
  version **135**

IKE SA
  aggressive mode **254**, **260**
  and certificates **259**
  and RADIUS **260**
  authentication algorithms **257**, **263**
  Diffie-Hellman key group **258**

  - encryption algorithms 257, 263
  - extended authentication 260
  - ID content 259
  - ID type 259
  - IP address, remote IPSec router 255
  - IP address, ZyXEL Device 255
  - local identity 259
  - main mode 254, 260
  - NAT traversal 261
  - negotiation mode 254
  - password 260
  - peer identity 259
  - pre-shared key 258
  - proposal 257
  - SA life time 262
  - user name 260
- IKE SA. See also VPN.
- incoming protocol filter 495
- Internet access setup 70, 497
- Internet Assigned Number Authority. See IANA.
- Internet Assigned Numbers AuthoritySee IANA 652
- Internet Protocol Security. See IPSec.
- IP address
  - assignment 498, 515
  - pool 135, 138, 173, 183, 493
  - private 134
- IP alias 495
- IP alias setup 495
  - DMZ 503
- IP protocol type 210
- IP static route 519
  - active 520
  - destination IP address 520
  - name 520
  - route number 520
- IPSec 253
- IPSec SA
  - active protocol 272
  - authentication algorithms 257, 263
  - authentication key (manual keys) 281
  - encapsulation 272
  - encryption algorithms 257, 263
  - encryption key (manual keys) 281
  - local and remote network any 270
  - local policy 270
  - manual keys 281
  - misconfiguration 270
  - nail up 262
  - Perfect Forward Secrecy (PFS) 273
  - proposal 273
  - remote policy 270
  - SA life time 262
  - Security Parameter Index (SPI) (manual keys) 281
  - transport mode 272
  - tunnel mode 272
  - when IKE SA is disconnected 262, 270
- IPSec SA. See also VPN.
- IPSec. See also VPN.
- ISP parameters 70

## L

- LAN 136
  - port filter setup 491
  - setup 491
- license key 129
- link type 59
- loading a configuration file 460
- log 562
- log and trace 562
- log facility 564
- login screen 468

## M

- MAC address 154, 482
- main menu commands 468
- maintenance 447
- Management Information Base. See MIB.
- managing subscription services 127
- managing the device
  - good habits 49
  - using FTP. See FTP.
  - using Telnet. See command interface.
  - using the command interface. See command interface.
- Max Age 147
- maximum incomplete high 214
- maximum incomplete low 214
- Media Access Control. See MAC address.
- menu overview 471
- metric 151, 349, 487, 513, 516, 520
- MIB 392
- multicast 135, 183, 488, 494, 516
- myZyXEL.com 127

## N

- nailed-up connection 512, 514
- NAT 134, 331, 340, 341, 487, 498, 515, 552, 652
  - and VPN 261
  - application 333

configuring 523
default server IP address 340
definitions 331
examples 530
how NAT works 332
in the SMT 521
inside global address 331
inside local address 331
Many to Many No Overload 334
Many to Many Overload 334
Many to One 334
mapping types 334
NAT unfriendly applications 536
One to One 334
ordering rules 526
port forwarding 340
port restricted cone 334
Server 335
server set 523
Single User Account 335
trigger port forwarding 537
what NAT does 332, 337

NAT traversal 261, 399
navigation panel 60
NBNS 136, 138
NetBIOS 138
NetBIOS Name Server. See NBNS.
Network Address Translation. See NAT.
Network Basic Input/Output System. See NetBIOS.
NTP time protocol 451

O

one minute high 214
one minute low 214
online services center 127
outgoing protocol filter 495
overlap in VPN 271

P

packet filtering 552
PAP 486, 513
parity 467
password 51, 448, 468
path cost 146
Perfect Forward Secrecy. see PFS.
PFS 273
  Diffie-Hellman key group 273
PIN number 129
ping 568
Point-to-Point Protocol over Ethernet. See PPPoE
Point-to-Point Tunneling Protocol. See PPTP.
pool of IP addresses 135, 138
port filter setup
  DMZ 501
  LAN 491
port forwarding 340
port restricted cone NAT 334
port statistics 64
Power Specification 613
PPPoE
  client 499
  encapsulation 71, 157, 497, 500, 510, 511, 512
  idle timeout 500
PPTP 73, 160
  Client 499
  configuring a client 499
  encapsulation 73, 160, 513
  idle timeout 499
private 349, 488, 516, 520
private IP address 134, 153
product overview 47
product registration 671
protocol filter 495
  incoming 495
  outgoing 495

R

RADIUS 323
  and IKE SA 260
  Shared Secret Key 324
RADIUS Message Types 323
RADIUS Messages 323
Rapid Spanning Tree Protocol. See Rapid STP.
Rapid STP 146
Real time Transport Protocol. See RTP.
registering your ZyWALL 128
registration
  product 671
related documentation 3
reload factory-default configuration file 53
remote management 378, 595
  CNM 396
  DNS 395
  FTP 391
  how SSH works 385
  HTTPS 378
  HTTPS example 380

  - limitations 378, 597
  - secure FTP using SSH 389
  - secure telnet using SSH 387
  - SNMP 392
  - SSH 385
  - SSH implementation 386
  - system timeout 378
  - Telnet 390
  - WWW 379
- remote node 509
  - filter 489, 516
- reports 425
  - host IP address 426, 427
  - protocol/port 426, 428
  - web site hits 426, 427
- required fields 469
- reset button 53
- resetting the time 452
- resetting the ZyWALL 53
- restore configuration 460, 577
  - via console port 584
- restoring factory defaults 461
- restoring files
  - via console port 579
  - via FTP 577
- retry count 485
- retry interval 485
- RFC 1058. See RIP.
- RFC 1305. See NTP time protocol.
- RFC 1389. See RIP.
- RFC 1466. See IP address.
- RFC 1597. See private IP address.
- RFC 1631. See NAT.
- RFC 1889. See RTP.
- RFC 2131. See DHCP.
- RFC 2132. See DHCP
- RFC 2402. See AH.
- RFC 2406. See ESP.
- RFC 3489. See STUN.
- RFC 867. See Daytime time protocol.
- RFC 868. See Time protocol.
- RIP 135, 488, 494, 495, 516
  - direction 135, 495
  - version 135, 495, 516
- Routing Information Protocol. See RIP.
- RSTP 146
- RTC 449, 591
- RTP 412

## S

- SA
  - life time 262
- safety warnings 6
- schedule 511, 514
  - duration 600
- scheduler 353
- screws 617
- secure FTP using SSH 389
- secure Telnet using SSH 387
- security associations. See VPN.
- security settings for VPN traffic 89
- server set 523
- service type 216, 498, 510
- services 127
- Session Initiation Protocol. See SIP.
- Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators. See STUN.
- Single User Account. See SUA.
- SIP 413
  - RTP 412
- SIP ALG 411
- skip VPN overlap 271
- SMT 467
  - changing the password 472
  - entering information 469
  - general setup 475
  - hidden menus 468
  - initial screen 467
  - login screen 468
  - main menu commands 468
  - menu overview 471
  - navigation 468
  - password 468
  - required fields 469
- SNMP 392
  - community 557
  - configuration 557
  - Get 393
  - GetNext 393
  - manager 392
  - MIB 392, 393
  - password 557
  - Set 393
  - Trap 393
  - trusted host 557
- source address 210, 230
- Spanning Tree Protocol. See STP.
- SSH 385
  - how SSH works 385
  - implementation 386
- stateful inspection firewall 191

static route **347**, **519**
stop bit **467**
STP **146**
  BPDU **146**
  Hello BPDU **147**
  how it works **146**
  Max Age **147**
  port states **147**
STUN **413**
SUA **521**
subnet **645**
subnet mask **133**, **646**
subnetting **648**
subscription services **127**
syntax conventions **4**
syslog logging **563**
system
  information **559**
  maintenance **559**
  name **447**, **475**
  status **559**
  timeout **378**
System Management Terminal. See SMT.

**T**

target market **47**
TCP maximum incomplete **214**
TCP/IP **514**
  and DHCP Ethernet setup **492**
  filter rule **546**
  setup **494**
Telnet **390**
terminal emulation **467**
TFTP
  configuration backup **575**
  file upload **582**
  GUI-based clients **575**
threshold **213**
time **449**
  and date setting **591**
  Daylight Saving Time **451**
  resetting **452**
  synchronization with server **452**
  zone **451**, **593**
Time protocol **451**
time protocol **451**
  Daytime **451**
  NTP **451**
  Time **451**
time setting **591**
timeout
  system **378**
trace **562**
trademarks **669**
traffic
  redirect **163**
transparent firewall **57**, **147**, **456**
triangle routes **202**
  vs virtual interfaces **202**
trigger port forwarding **537**
Trivial File Transfer Protocol. See TFTP.
troubleshooting **462**

**U**

unicast **135**
Universal Plug and Play. See UPnP.
upgrading firmware **457**
upload **583**
  firmware **579**
UPnP **399**, **400**
  examples **402**
  forum **400**
  NAT traversal **399**
  port mapping **401**
  UPnP Implementers Corp. **400**
user profiles **323**

**V**

Vantage CNM **395**
virtual address mapping over VPN **275**
virtual interfaces
  vs asymmetrical routes **202**
  vs triangle routes **202**
Virtual Private Network. See VPN.
VPN **160**, **253**
  active protocol **272**
  adjust TCP maximum segment size **288**
  and NAT **261**
  and the firewall **89**
  certificate **267**
  established in two phases **254**
  gateway policy **79**, **256**, **264**
  IKE SA. See IKE SA.
  IPSec **253**
  IPSec SA. See IPSec SA.
  local and remote network any **270**
  local network **253**
  local policy **270**
  misconfiguration **270**

    network policy **80**, **256**, **273**
    overlap **271**
    pre-shared key **267**
    proposal **257**
    remote IPSec router **253**
    remote network **253**
    remote policy **270**
    security associations (SA) **254**
    security on traffic **89**
    skip overlap **271**
    virtual address mapping **275**
VPN. See also IKE SA, IPSec SA.
VT100 terminal emulation **467**

## W

WAN
    file maintenance **574**
WAN DHCP **568**
WAN IP address **153**
WAN setup **481**
warranty **670**
    note **670**
web configurator **51**
web site hits **426**, **427**
Windows Internet Naming Service. See WINS.
WINS **136**, **138**
WINS server **138**
wireless channel **610**
wireless LAN **610**
wireless security **610**
wizard setup **69**
WLAN
    IP alias **506**
    setup **505**
    TCP/IP setup **506**
WWW **379**
www.dyndns.org **479**

## X

Xmodem **583**
    file upload **583**
    protocol **572**

## Z

ZyNOS **562**, **572**
ZyWALL registration **128**
ZyXEL’s Network Operating System. See ZyNOS.